

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p>					
1. REPORT DATE (DD-MM-YYYY)		2. REPORT TYPE Technical Report		3. DATES COVERED (From - To) -	
4. TITLE AND SUBTITLE A CONCEPTUAL FRAMEWORK FOR REPRESENTING HUMAN BEHAVIOR CHARACTERISTICS IN A SYSTEM OF SYSTEMS AGENT-BASED SURVIVABILITY SIMULATION				5a. CONTRACT NUMBER W911NF-10-1-0085	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER 611104	
6. AUTHORS Celestine Ntuen				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES North Carolina A&T State University 1601 East Market Street Greensboro, NC 27411 -0001				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211				10. SPONSOR/MONITOR'S ACRONYM(S) ARO	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) 57998-NS-H.1	
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT This research was conducted as a pilot study to model and simulate a mobile ad hoc network (MANET) as a system of systems (SoS) using selected human behavioral traits. A MANET as used in the research is a physics-based as well as a socio-technical system. As a socio-technical system (or human-machine system), multiple humans and multiple radios interact through some digital information connectivity. Thus, it is important to consider human behaviors in modeling and simulation of MANET systems in order to obtain useful performance metrics. It is observed that behavioral models are useful as MANETs seek to discover their neighbors through interconnection.					
15. SUBJECT TERMS Agents, Fuzzy matrix, MANET, Sociometrics					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			Celestine Ntuen
					19b. TELEPHONE NUMBER 336-285-3171

Report Title

A CONCEPTUAL FRAMEWORK FOR REPRESENTING HUMAN BEHAVIOR CHARACTERISTICS IN A SYSTEM OF SYSTEMS AGENT-BASED SURVIVABILITY SIMULATION

ABSTRACT

This research was conducted as a pilot study to model and simulate a mobile ad hoc network (MANET) as a system of systems (SoS) using selected human behavioral traits. A MANET as used in the research is a physics-based as well as a socio-technical system. As a socio-technical system (or human-machine system), multiple humans and multiple radios interact through some digital information connectivity. Thus, it is important to consider human behaviors in modeling and simulation of MANET systems in order to obtain useful performance metrics. It is observed that behavioral models are useful as MANETs seek to discover their neighbors through interconnection which are dependent on many social-behavioral factors such as trust and cooperation. In this project, a MANET is represented and modeled as a symmetric $n \times n$ fuzzy matrix. An algorithm for calculating the evolution behavior of MANET nodes using fuzzy product operations on the matrix is developed. It is shown that after a “sufficiently large number of iterations”, the fuzzy matrix converges to a “zero-one” matrix. The values of “0” and “1” simply means that two edges of the network with “1” have a crisp connectivity (and hence good communication), and those with “0” means no connectivity at all.

By conducting sample simulations using human behavioral variables, we were to discover the influences of sociometrics values (trust, cooperation, self-awareness, and shared information) in a MANET behavior. It is observed that as MANET nodes worked together and learned to know each other, the sociometrics values tended to increase connectivity with other nodes. For example, trust values between nodes increased. Further observed is the fact that a decrease in values for Cooperation and Self-awareness do not necessarily mean that there is a decrease in how the nodes cooperate or have self-awareness. It simply means that nodes with high cooperation and self-awareness were likely to share information and create more trust in the network as time evolved. This was achieved by incorporating behavior updating mechanisms into the simulation model.

The learning mechanism, using an equivalent of semantic distance metric, systematically trained the nodes (agents) in the MANET system to cooperate, trust, share information, and have self-awareness by adjusting their individual achievement weights from their sociometric scores. The learning model is characterized and derived by assuming that each agent in the MANET system can accommodate changes in its environment. This included its behavioral changes or perception of other agents based on the sociometric scale. For example, a learning score can be negative, zero, or positive. A negative score simply means that an agent has a reduced perception of other agents on the sociometric scales, a zero score means no change of opinion, and a positive score means a possible increase on the sociometric scales. A heuristic model for behavior adaptation was introduced into the sensitivity analyses using an “agent-follow-agent (AFA)” algorithm. AFA’s concept is simply: nodes with lower sociometric scores will seek to imitate the behaviors of nodes with high sociometric scores. A selfish node will not receive a follower, that is, it is insensitive to the needs of other nodes. For example, in our experiment, there was an agent that received 0% in adaptation score. This means that the agent does not have any trust, cooperate, or willing to share information with other agents. Any increase on followership scores indicate the ability of an agent to adapt to the environment as well as perceiving other agents with increase sociometric scores.

We experimented on the socio-metrics with an extension to how agents bind problems in context and provide solutions when faced with uncertainties and surprises such as those from non-authorized intrusion into the network. The focus was on how the socio-metric factors were used by MANET nodes when they encounter external emerging behaviors as opposed to learning the factors through connectivity algorithms. We found that agents interact and seek to self-organize when they experience a higher probability of intrusion into their domain. These issues are critical to the survivability of MANETS in battlefields. Thus, we can infer that when multiple entity behaviors interact, it is possible to derive emerging behaviors that make the functioning of a MANET scalable across different echelons of information abstraction and control.

REPORT DOCUMENTATION PAGE		Form Approved OMB NO. 0704-0188
Public Reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comment regarding this burden estimates or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188,) Washington, DC 20503.		
1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE November 22, 2010	3. REPORT TYPE AND DATES COVERED Technical Report: March 23, 2010- June 22, 2012
4. TITLE AND SUBTITLE A CONCEPTUAL FRAMEWORK FOR REPRESENTING HUMAN BEHAVIOR CHARACTERISTICS IN A SYSTEM OF SYSTEMS AGENT-BASED SURVIVABILITY SIMULATION		5. FUNDING NUMBERS W911NF-10-1-0085
6. AUTHOR(S) Celestine A. Ntuen, Ph.D		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Center for Human-Machine Studies North Carolina A&T State University 1601 East Market Street Greensboro, NC 27411		8. PERFORMING ORGANIZATION REPORT NUMBER 7N746
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U. S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211 Attn: Dr. S. Purushothaman Iyer		10. SPONSORING / MONITORING AGENCY REPORT NUMBER W911NF / N66020
11. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.		
12 a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution unlimited.		12 b. DISTRIBUTION CODE .

13. ABSTRACT (Maximum 200 words)

This research was conducted as a pilot study to model and simulate a mobile ad hoc network (MANET) as a system of systems (SoS) using selected human behavioral traits. A MANET as used in the research is a physics-based as well as a socio-technical system. As a socio-technical system (or human-machine system), multiple humans and multiple radios interact through some digital information connectivity. Thus, it is important to consider human behaviors in modeling and simulation of MANET systems in order to obtain useful performance metrics. It is observed that behavioral models are useful as MANETs seek to discover their neighbors through interconnection which are dependent on many social-behavioral factors such as trust and cooperation. In this project, a MANET is represented and modeled as a symmetric nxn fuzzy matrix. An algorithm for calculating the evolution behavior of MANET nodes using fuzzy product operations on the matrix is developed. It is shown that after a “sufficiently large number of iterations”, the fuzzy matrix converges to a “zero-one” matrix. The values of “0” and “1” simply means that two edges of the network with “1” have a crisp connectivity (and hence good communication), and those with “0” means no connectivity at all.

By conducting sample simulations using human behavioral variables, we were to discover the influences of sociometrics values (trust, cooperation, self-awareness, and shared information) in a MANET behavior. It is observed that as MANET nodes worked together and learned to know each other, the sociometrics values tended to increase connectivity with other nodes. For example, trust values between nodes increased. Further observed is the fact that a decrease in values for Cooperation and Self-awareness do not necessarily mean that there is a decrease in how the nodes cooperate or have self-awareness. It simply means that nodes with high cooperation and self-awareness were likely to share information and create more trust in the network as time evolved. This was achieved by incorporating behavior updating mechanisms into the simulation model.

The learning mechanism, using an equivalent of semantic distance metric, systematically trained the nodes (agents) in the MANET system to cooperate, trust, share information, and have self-awareness by adjusting their individual achievement weights from their sociometric scores. The learning model is characterized and derived by assuming that each agent in the MANET system can accommodate changes in its environment. This included its behavioral changes or perception of other agents based on the sociometric scale. For example, a learning score can be negative, zero, or positive. A negative score simply means that an agent has a reduced perception of other agents on the sociometric scales, a zero score means no change of opinion, and a positive score means a possible increase on the sociometric scales. A heuristic model for behavior adaptation was introduced into the sensitivity analyses using an “agent-follow-agent (AFA)” algorithm. AFA’s concept is simply: nodes with lower sociometric scores will seek to imitate the behaviors of nodes with high sociometric scores. A selfish node will not receive a follower, that is, it is insensitive to the needs of other nodes. For example, in our experiment, there was an agent that received 0% in adaptation score. This means that the agent does not have any trust, cooperate, or willing to share information with other agents. Any increase on followership scores indicate the ability of an agent to adapt to the environment as well as perceiving other agents with increase sociometric scores.

We experimented on the socio-metrics with an extension to how agents bind problems in context and provide solutions when faced with uncertainties and surprises such as those from non-authorized intrusion into the network. The focus was on how the socio-metric factors were used by MANET nodes when they encounter external emerging behaviors as opposed to learning the factors through connectivity algorithms. We found that agents interact and seek to self-organize when they experience a higher probability of intrusion into their domain. These issues are critical to the survivability of MANETS in battlefields. Thus, we can infer that when multiple entity behaviors interact, it is possible to derive emerging behaviors that make the functioning of a MANET scalable across different echelons of information abstraction and control.

14. SUBJECT TERMS Sensemaking, Personal Construct Theory, Collaborative Sensemaking, Complex Adaptive Information Systems, Judgment process, Tacit Knowledge, Naturalistic Decision Making process, Knowledge Creation and Discovery, Ecological Lens Model, Data/Frame Model, Finite State Automaton			15. NUMBER OF PAGES 90
			16. PRICE CODE
17. SECURITY CLASSIFICATION OR REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION ON THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL

Table of Contents Page

EXECUTIVE SUMMARY.....	6-8
DEFINITION OF TERMS.....	9
CHAPTER 1: Introduction to a mobile ad hoc mobile network as a system of systems	10-13
1.1. Background.....	10-11
1.2. MANET as a cognitive-physical system.....	11-12
1.3. Gaps and Challenges.....	12-13
1.4. Project Objectives.....	13
1.5. Chapter summary	13
CHAPTER 2: Related literature.....	10-19
2.1. Physical MANET systems: models and simulation.....	14-15
2.2. Cognitive MANET systems.....	16-18
2.3. Intelligent MANETS.....	18-19
2.4. Chapter summary.....	19
CHAPTER 3: Knowledge Action Network for MANET agents.....	20-30
3.1. A MANET model overview.....	20
3.2. A MANET as a dynamic graph.....	20-21
3.3. Knowledge action network for agents (KANA).....	21-29
3.4. Learning, predicting, and adaptation by a MANET nodes.....	29-30
3.5. Chapter summary.....	30
CHAPTER 4: Agent-based modeling and simulation of a cognitive MANET.....	31-41
4.1. Fondation of sociometrics for a cognitive MANET.....	31-32
4.2. Some challenges to sociometric development.....	32-33
4.3. Modeling socio-behavioral metrics in a MANET.....	33-34
4.4. Sociometric properties of a MANET.....	34-36
4.5. Simulation experiments.....	36-41
4.6. Chapter summary.....	41
CHAPTER 5: A sensitivity analyses of a MANET agent's use of sociometric for learning and adaptation.....	42-54
5.1. Background.....	42-43
5.2. Learning by MANET agents.....	43-51
5.3. Adaptation by MANET agents.....	51-54
5.4. Chapter summary.....	54
CHAPTER 6: A Laboratory simulation demonstration.....	55-58
6.1. A MANET configuration.....	55-56
6.2. Observations and sensitivity analysis.....	56-58
6.3. Chapter summary.....	58
CHAPTER 7: Summary, conclusions, and Lessons Learned for future Research.....	59-62
7.1. Summary and Conclusions.....	59-60
7.2. Lessons Learned.....	60-61

7.3. Suggestions for future research.....	61-62
References.....	63-68
Appendix A: More sociometric simulation results from Chapter 4.....	68-77

EXECUTIVE SUMMARY

This research was conducted as a pilot study to model and simulate a mobile ad hoc network (MANET) as a system of systems (SoS) using human behavioral traits.

In **Chapter 1**, we introduce a MANET as a physics-based system as well as a socio-technical system. As a SoS, each node in a MANET is a system by itself—having the ability to adapt, takes actions, and make decision in any battlefield situation. With its multiple node configurations, connectivity is the main conduit of a MANET system and can be decomposed into subsystems, each with different operational behavior.

In **Chapter 2**, a brief literature related to modeling and simulation of MANET systems from both physical and human behavioral model perspectives is presented. It is observed that behavioral models are useful as MANETs seek to discover their neighbors through interconnection which are dependent on many social-behavioral factors such as trust and cooperation. An important joint physical and behavioral property of a MANET is its mobility. Two primary types of mobility are commonly used: entity models, where the single nodes move independently of each other; and group mobility models, where some of the nodes are forming groups. The mobility is governed by certain randomly occurring behavioral factors such as task attractors (e.g., enemy pursuit) and fear of being identified by adversaries. Recent efforts on MANET modeling and simulation is the use of bio-inspired natural phenomena or using artificial neural network (ANN) models to help agents to dynamically learn routes in the network.

Chapter 3 presents fuzzy-based agent models for modeling a MANET behavior. A MANET is represented and modeled as a symmetric $n \times n$ fuzzy matrix. An algorithm for calculating the evolutionary behaviors of MANET nodes using fuzzy product operations on the matrix is developed. It is shown that after a “sufficiently large number of iterations”, the fuzzy matrix converges to a “zero-one” matrix. The values of “0” and “1” simply means that two edges of the network with “1” have a crisp connectivity (and hence good communication), and those with “0” means no connectivity at all. This property is used in the simulation to control result convergence and simulation termination.

Chapter 4 presents the results of modeling and sample simulations using human behavioral traits with the sociometrics as the dependent variables. It is observed that as MANET nodes learned to know each other, the sociometrics tended to increase the connectivity with other nodes. Further observed is the fact that a decrease in values for Cooperation and Self-awareness do not mean that there is a decrease in how the nodes cooperated or had self-awareness. It simply means that nodes with high cooperation and self-awareness are likely to share information and create more trust in the network as time evolved. This was achieved by incorporating behavior updating mechanisms into the simulation model. The learning mechanism systematically trains nodes in the MANET system to cooperate, trust, share information, and have self-awareness by adjusting their individual achievement weights from the sociometric scores.

Chapter 5 presents the results of sensitivity analyses for a MANET sociometric behavior using learning and adaptation policies. The learning model is characterized and derived by assuming that each agent in a MANET can accommodate changes in its environment. This included its behavioral changes or perception of other agents based on a sociometric scale. A learning score can be negative, zero, or positive. A negative score simply means that an agent has a reduced perception of other agents on the sociometric scales, a zero score means no change of opinion, and a positive score means a possible increase on the sociometric scales. A heuristic model for behavior adaptation is introduced into the sensitivity analyses using an “agent-follow-agent (AFA)” algorithm. AFA’s concept is simply: nodes with lower sociometric scores will seek to imitate the behaviors of nodes with high sociometric scores. A selfish node will not receive a follower since it is insensitive to the needs of other nodes. For example, in our experiment, Agent 10 was not receiving any followers (0% adaptation). This means that Agent 10 does not have any trust, cooperate, or willing to share information with other agents. Any increase on followership scores indicate the ability of an agent to adapt to the environment as well as perceiving other agents with increase sociometric scores. It also has some impacts on how actions are selected by the MANET nodes, especially connectivity decisions.

Chapter 6 mimicked a MANET behavior in a laboratory setting. We experimented on the socio-metrics with an extension to how agents bind problems in context and provide solutions when faced with uncertainties and surprises such as those from non-authorized intrusion into the network. The focus was on how the socio-metric factors were used when they encounter external emerging behaviors as opposed to learning the factors through connectivity algorithms. We found that agents interact and seek to self-organize when they experience a higher probability of intrusion into their domain. These issues are critical to the survivability of MANETs in the battlefields. Thus, we can infer that when multiple entity behaviors interact, it is possible to derive emerging behaviors that make the functioning of MANETs scalable across different echelons of information abstraction and control.

Lessons Learned

The following lessons are derived from the pilot study:

- (a). It is important to consider human behaviors in modeling and simulation of MANET systems in order to obtain useful performance metrics similar to socio-technical systems.
- (b). By conducting sample simulations using human behavioral variables, we were to discover the influences of sociometrics values (trust, cooperation, self-awareness, and shared information) in a MANET behavior.
- (c). It is observed that as MANET nodes learned to know each other, the sociometrics variables tended to increase, and so is the connectivity with other nodes.
- (d). Further observed is the fact that a decrease in values for Cooperation and Self-awareness do not necessarily mean that there is a decrease in how the nodes cooperate or have self-awareness. It simply means that nodes with high cooperation and self-awareness were likely to share information and create more trust in the network as time evolved.
- (e). The AFA algorithm was able to point to certain tendencies of selfish behaviors. For example, a selfish node will not receive a follower. In our model, Agent 10 was not

receiving any followers (0% adaptation). Any increase on followership scores indicate the ability of an agent to adapt to the environment as well as perceiving other agents with increase sociometric scores.

(f). Experiments to mimic a MANET in the laboratory also gave some useful information useful for design. We found that the agents interact and seek to self-organize when they experience a higher probability of intrusion into their domain. These issues are critical to the survivability of MANETS in battlefields.

Definition of Terms

AFA:	Agent-follow-agent
ANN:	Artificial neural network
ANT:	Actor network theory
DTC:	Decision tree classification
IEEE:	Institute for Electrical & Electronic Engineers
KANA:	Knowledge action network for agents
MANET:	Mobile ad hoc network
PMB:	Personal behavior model
QoS:	Quality of service
SHARC:	Stability and hop-count based algorithm for routing
SoS:	System of systems
UAJ:	Unattended jammer
UAV:	Unmanned aerial vehicles
WWW:	World wide web

CHAPTER 1

INTRODUCTION TO A MOBILE AD-HOC NETWORK AS A SYSTEM-OF SYSTEMS

1.1. Background

Modern battle command systems consist of a constellation of multiple networks of systems of people, organizations (e.g., Joint Task Forces, Coalition Forces, and Non-government organizations), weapon systems (ground vehicles, air vehicles, water vehicles, unmanned aerial, ground, and sea vehicles), multiple platform technologies and many support systems. This kind of battle command system has been referred to as a system of systems (SoS) (Bowman & Smith, 2009; Wegner, et al., 2006).

In the past, systems engineering techniques have been used for the architectural design of battle command systems from the standpoint of complexity theory. Here, complexity is defined primarily from interaction of structural and functional behaviors (Funge, Tu, & Terzopoulos, 1999). The contributions of the system engineering process can be summarized in terms of two related trends: (1) the increased importance of information processing and decision making and (2) the expanding complexity of large-scale systems-of-systems.

A SoS, as the name implies is an assemblage of different, stand-alone, heterogeneous systems in which the system goal is a weighted sum of the different subsystem goals. The system can be decomposed into subsystems that are simpler systems connected via their inputs and outputs. In a SoS metaphor it is assumed that each subsystem is an intelligent agent, with different behavior, capability, and skill. An event in a SoS starts with a single system, through change in behavior and affects the other systems state that are connected or interrelated with the affected system. Contrary to our familiarity with large-scale systems, a SoS is structured in a distributive design rather than a hierarchical design. Common examples of a SoS is the World Wide Web (WWW) which is reported to have over 320 million indexable pages containing over 15 billion words¹, and is growing at an astonishing rate. The major characteristics of a SoS are connected to many constructs such as behavior, emergence, adaptation, sharing, collaboration, and so on.

MANETs represent a class of tactical communication networks that are highly mobile and adaptive with respect to applications. MANETs also support robust and efficient operations, routing, communicating, and distributing information functionalities across their mobile nodes. MANET nodes may consist of laptops, Personal Digital Assistants (PDAs), tactical radios, or mobile phones with human beings as members of the nodes. An example MANET system is shown in Figure 1. These devices feature Bluetooth and/or IEEE 802.11 (Wi-Fi) network interfaces and communicate in a decentralized manner. Thus, MANETs represent cognitive socio-technical systems (CSTS) with intrinsic and extrinsic cognitive, perceptual, social and behavioral characteristics (Ntuen, Kim, Bowman, & Purush, 2011). However, current metrics for assessing the performance for MANETS are focused on the machine system properties such as vulnerability, resiliency, reliability, and energy use, quality of service, and speed

¹ Steve Lawrence and C. Lee Giles, "Searching the World Wide Web," *Science* **280**(3), 3 April 1998, pages 98 - 100

and accuracy of information processing.

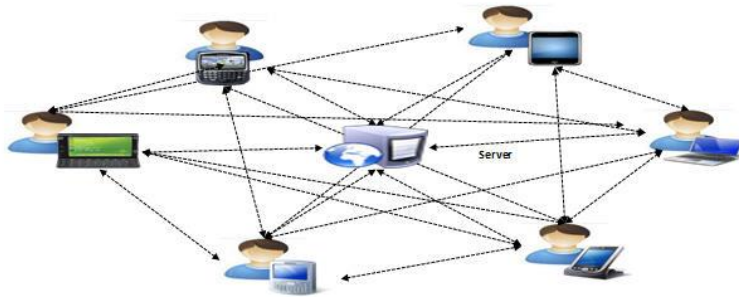


Figure.1. A simplified MANET topology.

1.2. A. MANET as A Cognitive-Physical System

Because humans are significant members of MANET systems, the physical properties alone are not sufficient to measure the system performance. For example, the analysts may need to know how agents (devices and humans) perceive the environment based on a MANET information load (voice, data, voice + data); how humans make decisions based on the tactical requirements as supported by MANET; how multiple humans and multiple MANET users interact; and how such interactions affect performance. Answers to these perceptual, cognitive, social, and behavioral questions lead to our interest in a computational approach to modeling, representing, and evaluating a MANET performance from a social and behavioral science stance. It is reasoned that designers and analysts of MANET systems should be cognizant of these multivariate performance dimensions to design cognitive MANETs (See Figure 2).

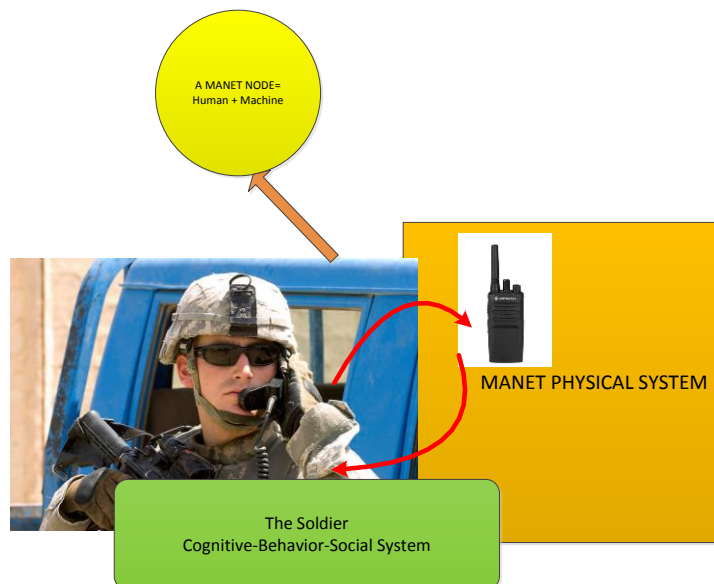


Figure 2. A single node MANET with a human and radio

The core technical challenge of our work involves tackling cross-disciplinary issues of a dynamic network protocol and multi-agent system design. An obvious approach is to build an agent out of two (or more) subsystems: a deliberative one, containing a symbolic world model, which develops plans and makes decisions in a rational manner; and a reactive one, which is capable of reacting to events that occur in the environment without engaging in complex reasoning. Often, the reactive component is given some kind of precedence over the deliberative one, so that it can provide a rapid response to important environmental events. Rather than the classical approach of symbolic reasoning, it is assumed here that agent's dynamic behavior is a result of interaction with other agents and the environment in which it works. The agent's ability to reason is not necessarily a sufficient condition for sensemaking, but the resultant behaviors arising from interactions—socially and ecologically.

The existing MANET models have failed to consider these social/psychological parameters of MANET simple because they are focused on the physical elements such as locations, routing, and battery energy. To add to modeling complexities, MANET nodes exhibit properties of human systems primarily because the human soldier is involved. Some of these human-like system properties are:

- (1) **Emergence**—the notion that the interaction of technological, cognitive, social, and ecological systems will give rise to a collective pattern of behaviors that differs remarkably from the presumed behaviors from each of sub-systems;
- (2) **Dynamic**—the notion that behavior change is situated in time and space given rise to temporal and spatial behaviors, respectively;
- (3) **Spiral model**—the notion that due to interactions of multiple behaviors, the resultant system behaviors are non-linear and information flow in the system and their functions is through a continuous spiral feedback model;
- (4) **Self-organized**—the notion that agents that have intelligent can adapt and re-organize their behaviors for planning during contingencies;
- (5) **Distributed cognition**—the notion that each agent in the system have the same situation awareness and seamlessly share what they know with each other;
- (6). **Sensemaking**—the notion that agents can reduce equivocal information to a common metric for use in an intended goal execution, and collectively seek prospective information for coping with future state changes (Ntuen, 2006);
- (7). **Agitative states**—the notion that MANET agents in the battlefield operate under stress levels which have the effect of diminishing the full functioning of the agent's performance such as reduction of awareness and attention

1.3 Gaps and Challenges

The first challenge in modeling a MANET with an agent-based system deals with adaptive behaviors as a consequent of information changes from battlefield tasks and the supporting mobile wireless communication networks. This challenge is important especially from the standpoint of knowledge management (Cioppa, 2003). The second challenge is reducing complicated and complex human observable behaviors to simple

qualitative rules for agents to learn. No real progress has been made in translating the relevant body of theories and paradigms in behavioral sciences into useful M&S models capable of empowering agents to recognize other agent behaviors and behave realistically in the domains of interest. Along the various dimensions of these challenges are gaps in the existing modeling constructs and frameworks. These are:

1. Agent models often are derived from the standpoint of system structures and functional properties (Dasilva & Srivasta, 2004).
2. There is a noticeable void in training agents to acquire behavior of other agents. This presents a problem in modeling a coalition of agents as a cooperative system.
3. Modeling concurrent behaviors in a MANET system requires sophisticated mathematical treatment than the current practice of using arbitrary interleaving models such as labeled transition systems.

1.4. Project Objectives

The following tasks are performed: (1) Conduct extensive literature review. (2) Develop an information rich framework that is computationally implementable for agent-based M&S environments with bias towards survivability modeling and simulation. (3) Clearly show the similarities and differences in agent characteristics with respect to how they perform at the physical, social, information, and cognitive levels of task abstractions. (4) Develop a prototype ontological model of the framework as a proof-of-concept in the battle command situation in which decision makers use a MANET.

1.5. Chapter 1 Summary

This chapter introduced a MANET as a physics-based system as well as a socio-technical system. As a SoS, each node in a MANET is a system by itself—having the ability to adapt, takes actions, and make decision in any battlefield volatile situation. With its multiple node configurations, connectivity is the main conduit of the system is viewed—from design and simulation perspectives. Thus a MANET can be decomposed into subsystems that are simpler systems connected via their outputs and inputs.

As a socio-technical system (or human-machine system), multiple humans and multiple MANET users interact through some digital information connectivity devices. Thus, it is surmised that human behaviors be used in modeling and simulation of MANET systems in order to obtain a useful performance metric. Such metrics include, perceptual, cognitive, social, and behavioral factors

CHAPTER 2

RELATED LITERATURE

2.1 Physical MANET Systems: Modeling and Simulation

A fundamental characteristic of mobile wireless networks is the time variation of the channel strength of the underlying communication links. Such time variation is due to multipath fading, path loss via distance attenuation, shadowing by obstacles, and interference from other users. By considering such variations, varieties of strategies have been proposed to evaluate a routing protocol in MANETs (Abolhasan, Wysocki and Dutkiewicz, 2004).

Quantitatively, some algorithms that evaluate a MANET performance based on the network connectivity are many in the literature (Abolhasan et al., 2004; Ammari and El-Rewini, 2004. Karhima, Lindroos, Hall and Haggman (2005) address the vulnerability of 802.11b (a set of IEEE standards that govern wireless networking transmission methods) based - MANETs due to intentional jamming by Unattended Jammer (UJ) and Unmanned Aerial Vehicle (UAV). These jammers use higher transmission powers than MANET nodes to obstruct the connectivity. Usually, the jammers are at locations through the simulation time span and have abilities to attack the MANET nodes based on the predefined combat power. For instance, connectivity may change even under nodes at fixed locations and configured with the same transmission power. The surrounding conditions other than location and transmission power factors could affect connectivity. Due to these drawbacks, link quality based routing methods (e.g. quality of service (QoS)) have been considered and used (Sridhar and Chan, 2005).

Link stability refers to the ability of a link to survive for a certain period. In this respect, link stability-based routing is unique to wireless networks. The stability of a link has a direct relationship to the distance and signal strength between two nodes. It depends on how long the two nodes remain within each other's communication range or signal strength is above a threshold. Sridhar and Chan (2005) proposed an algorithm called Stability and Hop-count based algorithm for Route Computing (SHARC) that uses hop-count and residual lifetime of the link as performance metrics. SHARC uses the shortest path algorithm by hop-count as the initial filter to narrow down route selections and then uses path stability by residual lifetime, a less robust indication, to choose the best route from among the available routes. Here, link stability is represented by the residual lifetime computed based on link age.

Link stability can be much more important in military MANETs during combat situations than in commercial networks since combat operations require a robust network connection to respond quickly and to maintain operational continuity. Because of these military aspects, some user nodes need to be supported with a higher priority than others are even though it may sacrifice network performance.

Routing is an important MANET performance measure. Routing is the mechanism of directing data packet flow from the source to the destination (Dengiz, 2007), and is very crucial in the MANET, because changes in a network topology and other states occur frequently and continuously. One common and traditional way of achieving routes in mobile Ad-hoc routing is to consider each host as a router (Buruhanudeen, Othman and Ali, 2007). There are three types of Ad-hoc mobile routing protocols, namely, Table

driven proactive, On-demand-driven reactive/Source initiated, and Hybrid protocols. Routing protocols react to any change in the topology even if no traffic is affected by the change, and they require periodic control messages to maintain routes to every node in the network. The rate at which these control messages are sent must reflect the dynamism of the network in order to maintain valid routes. Thus, the maintenance of the routing tables requires significant bandwidth (Chin, 2005). Representatives of this protocol category are:

- Destination-Sequenced Distance Vector Routing: each node maintains a list of all destinations and number of hops to each destination (Perkins and Bhagwat, 1994).
- Clustered Gateway Switch Routing Protocol: each node maintains a cluster member and a routing table (Chiang, 1997).
- Wireless Routing Protocol: each node maintains four tables; distance, routing, link cost and message retransmission list (Murthy and Garcia-Luna-Aceves, 1996).

Mobility is another important measure in a MANET, where it is assumed that nodes are free to move. The network topology and wireless link status are changed due to the mobility of nodes. Many different measures of mobility for evaluating mobile ad-hoc network performance have been proposed (He and Wei, 2008; Shukla, 2001). The most important characteristic of a mobility model is the degree of realism with respect to the movement of users, because models that are more realistic enable more accurate simulation and evaluation of network parameters. Kwak, Song and Miller, (2003) classify mobility models into stochastic and event-based group. They state that regardless of the selection of a mobility model, being able to measure the amount of mobility is as important as the realism of the model itself. To achieve the greatest realism, mobility modeling must take into consideration three essential factors (Stepanov, Maron, and Rothermel, 2005). These are spatial environments, user travel decisions, and user movement dynamism. Moreover, a mobility model must address both regular and random components of a user's movement.

Many authors have used different measures of mobility in their research. In Camp, Boleng, and Davies, (2002) and Shukla, (2001) the average speed of the nodes is used to represent their mobility, while the maximum speed is used by Ishibashi and Boutaba(2005) and Wilson (2001). The problem with using average or maximum speed as a measure of mobility is that the relative motion between the nodes is not reflected. In addition, the same average or maximum speed in different mobility models or in networks with different physical dimensions often results from different rates of route changes (Kwak, Song, and Miller, 2003).

Interoperability is another measure of a MANET performance. An example of this interoperability occurs in a disaster scenario where several teams of first responders (fire fighters, ambulance teams, police officers, etc.) are deployed to the scene of a disaster and cooperate to save lives and property. Each team of first responders may have its own network of handheld devices. Often, effective disaster management plans require that the teams be able to share information among each other despite the heterogeneous hardware and software profiles of their networks.

2.2 Cognitive MANET Systems

Thomas et al. (2005) define a cognitive network as having a cognitive process that is capable of perceiving current network conditions and then planning, deciding, and acting on those conditions. Cognitive networks are able to reconfigure the network infrastructure based on past experiences by adapting to continuously changing network behaviors to improve scalability (e.g., reducing complexity), survivability (e.g., increasing reliability), and QoS level (e.g., facilitating cooperation among nodes) as a forward looking mechanism.

Tan, Zhou, Ho, Mehta, & Tanabe, (2002) use a game theoretic approach to analytically model node behaviors in voluntary resource sharing networks and quantify the cost/benefit tradeoffs that will lead nodes to volunteer their resources. A game theoretic approach was used due to its applicability to modeling conflict and cooperation among rational decision-makers. In their design, it is assumed that group movement is the result of interaction between behaviors of individual nodes in a MANET. While each node acts separately from all other entities around it, its decisions are somehow affected by the context it is in and by the movement surrounding it.

There are three sub-models that define the model: the perception sub-model (what each node “sees”), the behavioral sub-model (what each node infers from the information available), and the movement sub-model (how each node actually moves). The perception model tries to make available to the behavioral model approximately the same information that is available to a real human as the end result of its perceptual and cognitive processes. The behavioral model takes this information and decides how it should move based on current state, user parameters, and system defined parameters. The movement model takes input from the behavioral model and calculates the actual movement of the nodes so as to keep a consistent state of the world.

Daly & Haahr (2007) developed a multidisciplinary solution based on the consideration of the so called small world dynamics which have been proposed for economy and social studies and have recently revealed to be a successful approach to be exploited for characterizing information propagation in wireless networks. To this purpose, some bridge nodes are identified based on their centrality characteristics, i.e., on their capability to broker information exchange among otherwise disconnected nodes. Musolesi & Mascolo (2007) employed social network analysis to study node relationships in a MANET type communication network. The weights associated with each edge of the social network are used to model the strength of the interactions between nodes. Their model studied the degree of social interaction between communication nodes using a value in the range $[0, 1]$; with 0 indicating no interaction and 1 indicates a strong social interaction.

Hui, Crowcroft, & Yonek (2008) developed BUBBLE Rap, a software agent that combines the knowledge of community structure with the knowledge of node centrality to make forwarding decisions. There are two intuitions behind this algorithm. Firstly, people have varying roles and popularities in society, and these should be true also in the network – the first part of the forwarding strategy is to forward messages to nodes which are more popular than the current node. Secondly, people form communities in their social lives, and this should also be observed in the network layer – hence the second part of the forwarding strategy is to identify the members of destination communities, and to use them as relays.

Wei & Guosun (2010) used a cognitively-inspired method from the brain informatics (BI) to investigate the search efficiency and scalability of MANETs by clustering nodes based on cognitive trust mechanism. The trust relationship is formed by evaluating the level of trust using Bayesian statistical analysis, and clusters can be formed and maintained autonomously by nodes with only partial knowledge. Simulation experiments show that each node can form and join proper clusters, which improve the interaction performance of the entire network. Liu et al. (2004) proposed a trust model by monitoring the behavior of neighbors and recommendations received from them. Pirzada et al. (2004) proposed a similar approach for establishing trusted routes in dynamic source routing. Virendra et al. (2005) proposed a trust model to establish group keys in a MANET using trust relationships that exist among nodes.

Based on an extensive survey of trust in a MANET, Cho & Swani (2009) observed the following characteristics:

1. A decision method to determine trust against an entity should be fully distributed since the existence of a trusted third party (such as a trusted centralized certification authority) cannot be assumed.
2. Trust should be determined in a highly customizable manner without excessive computation and communication load, while also capturing the complexities of the trust relationship.
3. A trust decision framework for MANETs should not assume that all nodes are cooperative. In resource-restricted environments, selfishness is likely to be prevalent over cooperation, for example, in order to save battery life or computational power.
4. Trust is dynamic, not static.
5. Trust is subjective.
6. Trust is not necessarily transitive. The fact that A trusts B and B trusts C does not imply that A trusts C.
7. Trust is asymmetric and not necessarily reciprocal.
8. Trust is context-dependent. A may trust B as a wine expert but not as a car fixer. Similarly, in MANETs, if a given task requires high computational power, a node with high computational power is regarded as trusted while a node that has low computational power but is not malicious (i.e., honest) is distrusted.

Frias-Martinez, et al. (2009) developed *BARTER*, a mechanism that automatically creates and updates admission and access control policies for MANETs based on behavior profiles. In *BARTER* protocol, MANET members initially exchange their behavior profiles and compute individual local definitions of normal network behavior. Behavior is used to represent the typical communications of network devices i.e., the traffic payload observed or specific volumetric measurements of the traffic such as average number of packets. The decision of each individual MANET member is based on the accumulation of knowledge gathered from the behavior profiles of other members. Djenouri & Badache (2008) noted that a typical MANET has a selfish behavior. This is a result of the limitation in energy resources along with the multi-hop nature of MANETs. To preserve its own battery, a node may behave selfishly and would not forward packets originated from other nodes, while using their services and consuming their resources.

Prema, et al. (201) advocated the use of personal behavior model (PBM) to simulate the dynamics of MANET nodes. Dynamic behaviors are defined as the intended real movement patterns of individual nodes in the environment based on the activities to be performed in the different attraction points. PBM is formulated by means of a bi-nary matrix formed based upon the practical scenario and node based inputs at a particular time interval.

Actor-network theory (ANT) from Bruno Latour (1992) provides some theoretic foundations to modeling MANET systems from social science perspectives. ANT analysis describes the progressive constitution of a network in which both human and non-human actors assume identities according to prevailing strategies of interaction. Actors' identities and qualities are defined during negotiations between representatives of human and non-human actants. In this perspective, "representation" is understood in its political dimension, as a process of delegation. The most important of these negotiations is "translation," a multifaceted interaction in which actors (1) construct common definitions and meanings, (2) define representatives, and (3) co-opt each other in the pursuit of individual and collective objectives. In the actor-network theory, both actors and actants share the scene in the reconstruction of the network of interactions leading to the stabilization of the system. But the crucial difference between them is that only actors are able to put actants in circulation in the system.

2.3 Intelligent MANETs

An artificial neural network (ANN) is among the oldest techniques in machine learning. Farago, Myers Syrotiuk and Zarub (2000) applied ANN in their meta medium access layer (meta-MAC) network. Benaissa, Lecuire, Syrotiuk and McClary (2004) have examined potential applications of decision classification for the transport of voice in a mesh network. Dowling, Curran, Cunningham and Cahill (2005) have applied reinforcement learning and some elements of ant colony optimization to multi-hop routing in MANETs. McClary, Syrotiuk and Lecuire (2007) have examined the use of artificial neural networks for multimedia transport in MANETs. Colagrosso (2005, 2006) applied Bayesian classifiers to MANET broadcasting, targeting both packet construction, and rebroadcasting. Kazantzidis (2005) has examined potential applications for medium access control. Malpani, Chen, Vaidya and Welch (2005) employed decision tree classification (DTC). Liu, Li and Man (2005) used DTC in their recent MAC-layer intrusion-detection work on a MANET. Kaaniche and Kamoun (2010) proposed a recurrent neural network for long-term time series prediction, since mobility prediction is a particular problem of time series prediction.

Vicente, Dorgham and Radu (2005) designed a self-organizing routing algorithm called NEURAL achieved using classification, adaptive and learning algorithms from the artificial neural system. This routing protocol inspired by the synapses in the brain, in which neighbor neurons compete to propagate the signal. Knoester, Goldsby and McKinley (2010) demonstrated that neuroevolution can discover distributed behaviors for mobile sensor networks. Neuroevolution is a population of ANNs subject to mutation and natural selection.

Among methods, paradigms available to simulate, and model MANETs, agents and multi-agent systems are receiving more attention. Agent's autonomy can be regard as ad hoc in MANET and the mobility of network nodes being interpreted in terms of

mobility of agents. Pickman, (2008) presents a low cost simulator to the system designer and developer. The low cost mobile node network simulator is based on open source software and commercial-off-the-shelf hardware elements, which provide low cost, adaptable, and loosely coupled simulator for modeling, and simulating mobile node networked systems. Gaines and Ramkumar (2008) proposed a framework for dual agent secure routing protocols where every mobile device consists of an untrusted user agent and a trustworthy network agent with modest capabilities. The network agents are constrained to perform only symmetric cryptographic computations and efficiently reuse a single hardware block cipher. The network agent strives to keep the user agent (all other components of the mobile device) in check to ensure adherence to the rules to be followed for co-operative routing. This leads to taxonomy of attacks and low complexity strategies well within the scope of network agents to address such attacks. Marwaha and Indulska (2011) present an algorithm that used distributed cooperative mobile agents for routing in dynamic networks such as MANETs. It is bio-inspired, utilizing ant-like mobile agents in MANET.

2.4. Chapter Summary

This chapter presented a brief literature related to modeling and simulation of MANET systems from both physical and human behavioral model perspectives. Behavioral models are useful as MANETs seek to discover their neighbors through interconnection which are dependent on many social-behavioral factors such as trust and cooperation. Cho & Swani (2009) suggested that by combining notions of “social trust” derived from social networks with “quality-of-service (QoS) trust” derived from communication networks, we can obtain a composite trust metric for a MANET. Zouridaki, et al. (2006) noted used trust to induce cooperation between MANET nodes. In their proposed schemes, first-hand trust information is obtained independently of other nodes and second trust information obtained via recommendations from other nodes. The method exploits information sharing among nodes to accelerate the convergence of trust establishment

An important joint physical and behavioral property of a MANET is its mobility. Two primary types of models are common, entity models, where the single nodes move independently of each other; and group mobility models, where some of the nodes are forming groups. This mobility is governed by certain randomly occurring behavioral factors such as task attractors (e.g., enemy pursuit or concealment from the enemy) and fear of being identified by adversaries. Recent efforts on a MANET modeling and simulation is the use of bio-inspired natural phenomena or using ANN models to help agents to dynamically learn routes in the network.

CHAPTER 3

KNOWLEDGE ACTION NETWORK FOR MANET AGENTS

3.1. A MANET Model Overview

In MANET, nodes communicate via wireless *links*. Each node has a limited transmission range. We assume that two nodes are connected with each other if the distance between them is smaller than the maximum of their transmission range. That is if tr_A and tr_B are transmission ranges of agent A and B respectively; A and B are connected if and only if $d(A, B) \leq \max(tr_A, tr_B)$. All the links in the network are bi-directional however, connections between nodes is asymmetric. The level to which an agent A is connected to another agent B is different from the level of B to A (Figure 3).

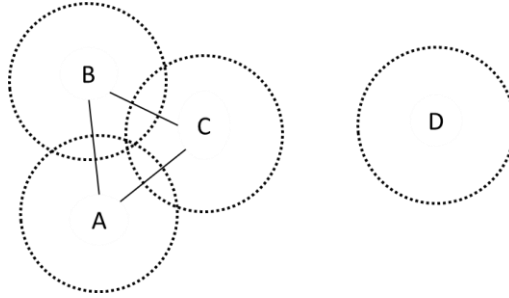


Figure 3. MANET node connections with illustrative spheres of influence through transmission range interactions.

A MANET topology is dynamic because the connectivity among the nodes changes as they are moving. While moving, the nodes can stay connected to other nodes but they can also be completely without neighbors. They can move everywhere within this area but they are unable to go out of this area and no new nodes can enter the network. A node in the network will always know who its neighbors are. Therefore, while moving, a node will immediately know its new neighbors. In this project, a MANET node is referred as an agent.

3.2. A MANET as A Dynamic Graph

A MANET is a network and thus can be represented as a graph, G . $G = (X, E)$ is a collection X of vertices or nodes together with a collection E of edges. The graph is finite if it has finitely many vertices and edges. Each edge has either one endpoint, $\text{end}(e) = \{x\}$ in which case e is termed a loop at vertex x , or two endpoints, $\text{end}(e) = \{x, y\}$ in which case e is termed a link between vertices x and y . A graph is simple if it is loop-free or each edge is a link, and has no multiple edges: $\text{end}(e_1) = \text{end}(e_2) \Rightarrow e_1 = e_2$.

An edge of a simple graph may be identified with the pair of its endpoints. The adjacency matrix of a finite graph G with n vertices is the $n \times n$ matrix where the non-diagonal entry a_{ij} is the number of edges from vertex i to vertex j , and the diagonal entry a_{ii} , depending on the convention, is either once or twice the number of edges (loops) from vertex i to itself.

$G' = (X', E')$ is a **subgraph** of $G = (X, E)$ if $X' \subseteq X, E' \subseteq E$, and the mappings that send an edge $e \in E'$ to its endpoints in G' and in G coincide. G' spans G if $X' = X$; a spanning tree of G is a subgraph, which is a tree spanning G . An orientation of an edge e is an ordered pair of vertices (x, y) such that $\text{end}(e) = \{x, y\}$, thus a loop at x has only one possible orientation: (x, x) , while a link between x and y has two possible orientations, (x, y) and (y, x) .

Ferreira and Jarry, (2003) proposed a model that stores the different events changing the behaviors in a graph during its evolution. The result is a static graph containing all edges and all vertices that existed during the evolution life cycle of the observed graph. The edges are labeled with information about events of evolution.

Let $G = (V, E)$ be a directed graph with V a set of vertices and E a set of arcs whose endpoints belong to V . $SG = \{G_1, G_2, \dots, G_T\}$, a set of subgraphs of G . The system $G = (G, S_G)$ is called "evolving graph".

This definition corresponds to a graph model allowing the aggregation of a list of static subgraphs. Each graph represents the state of the studied network at one instant. This is shown in Figure 4 below. Each subgraph can consist of any number of vertices and edges, the model handles the dynamic topology of the network (adding or removing vertices and edges), and it can also represent the changes in valuations on vertices and edges.

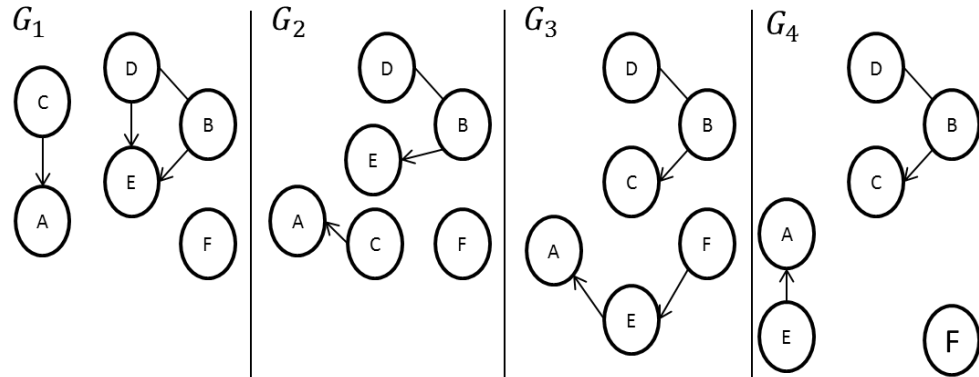


Figure 4. Example of static graphs representing four evolution stages of a dynamic graph

3.3. A Knowledge Action Network for Agents (KANA)

The design of Agent-Based Simulations (ABSs) is based on the idea that it is possible to develop a computerized form of entity behaviors in a system which is active in the world. The implication is that, such a model can capture an emergent collective behavior from interacting behaviors of the entities. While good results are achieved, it is noted by Sabater & Sierra (2002) that this idea is simplified by assuming that agents will use psychological models to operate independently in perceiving the simulated world and in forming their reactions to it. The collection of algorithms to represent perception, cognition, actions in a MANET is referred to here as a Knowledge Action Network for Agents (KANA). KANA is designed to capture how knowledge is used by agents to achieve intended system-level actions. Capturing the knowledge entails the formalization of mathematical algorithms to represent, say, social behaviors, interactions, collaborations and information sharing among entities in a system.

The first part of KANA is understanding node connectivity in a MANET. Traditionally, researchers look at graph or network connectivity in two ways—as either vertex connectivity or edge connectivity. Connectivity in ad-hoc networks has been studied previously by Penrose (1999). In this work, a fuzzy connectivity matrix is used for knowledge capture and representation to study node connectivity. As an illustration, consider a five node MANET layout with its regions of connectivity (Figure 5). First, the fuzzy connectivity matrix is determined. To do this, an algorithm based on disk geometry representation is developed. The disk geometry representation is like a Venn diagram of regions of access (RoA). That is, for two disks; a distance metric of information transmission using RoA is calculated. The algorithm is given in equation 1.

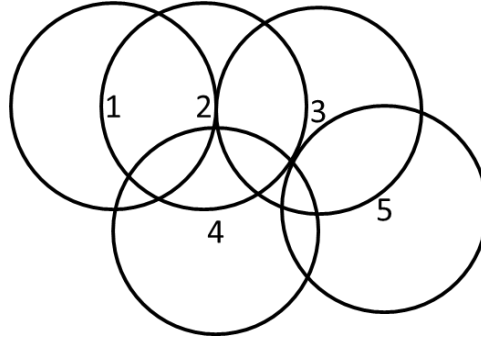


Figure 5. Five nodes MANET example.

$$a_{ij} = \begin{cases} r_i^2 \cos^{-1} \left(\frac{d_{ij}^2 + r_i^2 - r_j^2}{2d_{ij}r_i} \right) + r_j^2 \cos^{-1} \left(\frac{d_{ij}^2 + r_j^2 - r_i^2}{2d_{ij}r_j} \right) - \\ \frac{1}{2} \sqrt{(-d_{ij} + r_i + r_j)(d_{ij} - r_i + r_j)(d_{ij} + r_i - r_j)(d_{ij} + r_i + r_j)} & \text{if } d_{ij} \neq 0 \dots\dots(1) \\ \pi r_i^2 & \text{if } d_{ij} = 0 \text{ and } r_i \leq r_j \\ \pi r_j^2 & \text{if } d_{ij} = 0 \text{ and } r_j \leq r_i \end{cases}$$

In Equation 3.2, r_i is the radius of node i , d_{ij} is the Euclidean distance between node i and node j ; and the algorithm uses the “Circle-Circle Intersection” of Weisstein available online: (<http://mathworld.wolfram.com/Circle-CircleIntersection.htm>). As an example, consider a two-node MANET below in Figure 6. Assume that $d_{12} = 1$, $r_1 = 0.5$ and $r_2 = 0.75$, then

$$\begin{aligned} a_{12} &= (0.5)^2 \cos^{-1} \left(\frac{1^2 + 0.5^2 - 0.75^2}{2 \times 0.5} \right) + (0.75)^2 \cos^{-1} \left(\frac{1^2 - 0.5^2 + 0.75^2}{2 \times 0.75} \right) \\ &- \frac{1}{2} \sqrt{(-1 + 0.5 + 0.75)(1 - 0.5 + 0.75)(1 + 0.5 - 0.75)(1 + 0.5 + 0.75)} \end{aligned}$$

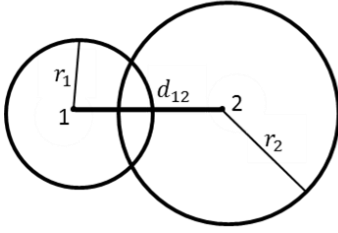


Figure 6. An example of a two-node network.

$$\begin{aligned}
 &= 0.25 \times \cos^{-1}(0.6875) + 0.5675 \times \cos^{-1}(0.875) - \frac{1}{2} \sqrt{(0.25)(1.25)(0.75)(2.25)} \\
 &= 0.25 \times (0.8127) + 0.5675 \times (0.5054) - 0.3631 \\
 &a_{12} = 0.1269
 \end{aligned}$$

Definition 1: Let x_1 be a node with center 1 and radius r_1 and x_2 the node with center 2 and radius r_2 , then we define the fuzzy connectivity from x_1 to x_2 (denoted $x_1 \longrightarrow x_2$) to be $\frac{a_{12}}{\pi r_1^2}$. Similarly, $x_2 \longrightarrow x_1 = \frac{a_{12}}{\pi r_2^2}$.

For the sample network, $x_1 \longrightarrow x_2 = \frac{0.1269}{3.14 \times 0.25} = 0.1616$

$$x_2 \longrightarrow x_1 = \frac{0.1269}{3.14 \times 0.25} = 0.0718$$

As another illustration, consider four agents x_1, x_2, x_3 and x_4 respectively located at the geometric points, (5,3), (5,3), (5,6) and (4,7) with radius 4, 5, 6 and 3. The fuzzy connectivity matrix Z is calculated as

$$Z = \begin{bmatrix} 1 & 1 & 0.8936 & 0.2223 \\ 0.6400 & 1 & 0.7807 & 0.2226 \\ 0.3971 & 0.5421 & 1 & 0.2500 \\ 0.3952 & 0.6185 & 1 & 1 \end{bmatrix}$$

To model MANET evolutionary behaviors, the following definitions are necessary:

Definition 2: Given two nodes (agents) with labels, i and j , a path from i to j is a sequence of transitions that beginning in i and ends in j , such that each transition in the sequence has a positive probability of occurring.

Definition 3: An agent j is reachable from agent i if there is a path leading from i to j .

Definition 4: Two agents i and j are said to communicate if j is reachable from i , and i is reachable from j .

Definition 5: A set of agents in a MANET S is a closed set if no agent outside of S is reachable from any state in S .

Agent nodes may be partitioned into separate classes (sets) such that the agents that communicate with each other are in the same class. If there is only one class, the MANET is said to be fully connected. A MANET communication could be explained using its connectivity matrix. Algebraically, the entry of connectivity matrix indicated how good is the connection between agent i and agent j . Ultimately, an internal action will let a MANET evolve to a single node, that is after certain exchange of information

all agents have the same knowledge. In a matrix form, there exists an integer, such that; ones (n) are a matrix of dimension n of all 1.

Proposition 1: If a MANET is fully connected, and nodes are only involved in communication action; i.e., there is no node movement; it will end up after a certain time behaving as a single node. In other words if a MANET is represented by its fuzzy connectivity matrix A; it exists an $n \in \mathbb{N}$, such that $A^n = \text{ones}(n)$.

Proof

Let $A = (a_{ij})_{1 \leq i, j \leq n}$ a full MANET connectivity matrix; let $A^k = (a_{ij}^k)$ be the k- power of A. We will prove that:

$(a_{ij}^k)_{k \in \mathbb{N}}$ is an increasing and bounded sequence; hence converging.

$a_{ij}^k = \bigoplus_{l=1}^n (a_{il}^{k-1} \otimes a_{lj}^{k-1})$; in this “sun” the term when $l = j$ is $a_{ij}^{k-1} \otimes a_{jj}^{k-1} = a_{ij}^{k-1}$ because $a_{jj}^{k-1} = 1$. We thus have $a_{ij}^{k-1} \leq a_{ij}^k$. $a_{ij}^k \leq 1$ for all $1 \leq i, j, k \leq n$.

Definition 6: (Addition of fuzzy matrices). Giving two fuzzy matrices $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ and $B = (b_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}}$ representing two configurations of MANET nodes, if

$\text{dimension}(A) = \text{dimension}(B)$ i.e., $m = r$ and $n = s$, then a fuzzy addition $A \oplus B$ is defined as $A \oplus B = (c_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ where $c_{ij} = \max(a_{ij} + b_{ij}, 1)$ is the Lukasiewicz t-conorm.

Definition 7: (multiplication of fuzzy matrices) Giving two fuzzy matrices

$A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ and $B = (b_{ij})_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}}$, if $\text{dimension}(A, 2) = \text{dimension}(B, 1)$ i.e., $n = r$

then a fuzzy multiplication $A \otimes B$ is defined as $A \otimes B = (c_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$; where

$c_{ij} = \bigoplus_k (a_{ik} \otimes b_{kj})$ and $a \otimes b = \max(a + b - 1, 0)$ is the Lukasiewicz t-norm and the associated Lukasiewicz t-conorm is defined by $a \oplus b = \min(1, a + b)$.

In the formula for fuzzy matrices multiplication, one can replace Lukasiewicz t-conorm and Lukasiewicz t-norm by any other t-conorms and its associate t-norms. Examples of such t-norms and the associated t-conorms are giving Table 1 below.

Note that for a t-norm \top , its associated t-conorm \perp can be defined as

$$\perp(a, b) = 1 - \top(1 - a, 1 - b) \quad (2)$$

The example with matrices A and B illustrate the sample calculations.

$$\text{Let } A = \begin{bmatrix} 0.8 & 0.4 & 0.5 \\ 0.5 & 0.9 & 0.1 \\ 0.6 & 0.6 & 0.3 \end{bmatrix} \text{ and } B = \begin{bmatrix} 0.7 & 0.2 & 0.5 \\ 0.6 & 0.6 & 0.4 \\ 0.8 & 0.1 & 0 \end{bmatrix}$$

Table 1. Sample fuzzy t-norms and t-conorms (Klir & Folger, 1998)

t-norm	t-conorm
Minimum t-norm $\mathbb{T}_{min}(a, b) = \min(a, b)$	Maximum t-conorm $\perp_{max}(a, b) = \max(a, b)$
Product t-norm $\mathbb{T}_{prod}(a, b) = a \cdot b$	Probabilistic sum $\perp_{sum}(a, b) = a + b - ab$
Lukasiewicz t-norm $\mathbb{T}_{Luk}(a, b) = \max(0, a + b - 1)$	Bounded sum $\perp_{Luk}(a, b) = \min(1, a + b)$
Drastic t-norm $\mathbb{T}_D(a, b) = \begin{cases} b & \text{if } a = 1 \\ a & \text{if } b = 1 \\ 0 & \text{otherwise} \end{cases}$	Drastic t-conorm $\perp_D(a, b) = \begin{cases} b & \text{if } a = 0 \\ a & \text{if } b = 0 \\ 1 & \text{otherwise} \end{cases}$
t-norm	t-conorm
Nilpotent minimum $\mathbb{T}_{nM}(a, b) = \begin{cases} \min(a, b) & \text{if } a + b > 1 \\ 0 & \text{otherwise} \end{cases}$	Nilpotent maximum $\perp_{nM}(a, b) = \begin{cases} \max(a, b) & \text{if } a + b < 1 \\ 0 & \text{otherwise} \end{cases}$
Hamacher product $\mathbb{T}_{H_0}(a, b) = \begin{cases} 0 & \text{if } a = b = 0 \\ \frac{ab}{a+b-ab} & \text{otherwise} \end{cases}$	Einstein sum $\perp_{H_2}(a, b) = \frac{a+b}{1+ab}$

For addition (\oplus):

$$A \oplus B = \begin{bmatrix} 0.8 \oplus 0.7 & 0.4 \oplus 0.2 & 0.5 \oplus 0.5 \\ 0.5 \oplus 0.6 & 0.9 \oplus 0.6 & 0.1 \oplus 0.4 \\ 0.6 \oplus 0.8 & 0.6 \oplus 0.1 & 0.3 \oplus 0 \end{bmatrix} = \begin{bmatrix} 1 & 0.6 & 1 \\ 1 & 1 & 0.5 \\ 1 & 0.7 & 0.3 \end{bmatrix}$$

For multiplication (\otimes):

$$\begin{aligned}
A \otimes B &= \begin{bmatrix} (0.8 \otimes 0.6) \oplus (0.4 \otimes 0.6) \oplus (0.5 \otimes 0.8) & (0.8 \otimes 0.2) \oplus (0.4 \otimes 0.6) \oplus (0.5 \otimes 0.1) & (0.8 \otimes 0.5) \oplus (0.4 \otimes 0.4) \oplus (0.5 \otimes 0) \\ (0.5 \otimes 0.6) \oplus (0.9 \otimes 0.6) \oplus (0.1 \otimes 0.8) & (0.5 \otimes 0.2) \oplus (0.9 \otimes 0.6) \oplus (0.1 \otimes 0.1) & (0.5 \otimes 0.5) \oplus (0.9 \otimes 0.6) \oplus (0.1 \otimes 0) \\ (0.6 \otimes 0.6) \oplus (0.6 \otimes 0.6) \oplus (0.3 \otimes 0.8) & (0.6 \otimes 0.2) \oplus (0.6 \otimes 0.6) \oplus (0.3 \otimes 0.1) & (0.6 \otimes 0.5) \oplus (0.6 \otimes 0.6) \oplus (0.3 \otimes 0) \end{bmatrix} \\
&= \begin{bmatrix} ((0.4)) \oplus (0) \oplus (0.3) & (0) \oplus (0) \oplus (0) & (0.3) \oplus (0) \oplus (0) \\ (0.1) \oplus (0.5) \oplus (0) & (0) \oplus (0.5) \oplus (0) & (0) \oplus (0.5) \oplus (0) \\ (0.2) \oplus (0.2) \oplus (0.1) & (0) \oplus (0.2) \oplus (0) & (0.1) \oplus (0.2) \oplus (0) \end{bmatrix} \\
&= \begin{bmatrix} 0.8 & 0. & 0.3 \\ 0.7 & 0.5 & 0.3 \\ 0.6 & 0.2 & 0.1 \end{bmatrix}
\end{aligned}$$

$$\text{Similarly, } B \otimes A = \begin{bmatrix} 0.6 & 0.3 & 0.2 \\ 0.5 & 0.5 & 0.1 \\ 0.6 & 0.2 & 0.3 \end{bmatrix}$$

Note that $A \otimes B \neq B \otimes A$ meaning that multiplication of fuzzy matrix is not commutative.

Proposition 2: Fuzzy square matrices have the special property that for every fuzzy square matrix A , there exist $n \in \mathbb{N}$ such that $A^{n+1} = A^n$. That is, the relational matrix $A_{n \times n}$ induced by n -node MANETs, after a period of sharing information, will likely have a converging behavior. That is matrix A is stationary.

Proof: Let $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ be a fuzzy square matrix of size n .

Case 1. $(\forall 1 \leq i, j \leq n), a_{ij} < \frac{n}{(2n-1)}$, then letting $A^2 = (c_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$,

$$c_{ij} = (a_{i1} \otimes a_{1j}) \oplus (a_{i2} \otimes a_{2j}) \oplus \dots \oplus (a_{in} \otimes a_{nj})$$

$$a_{ik} \otimes a_{kj} = \max(0, a_{ik} + a_{kj} - 1) < \max\left(0, \frac{2n}{(2n-1)} - 1\right) = \frac{1}{(2n-1)}$$

$$\Rightarrow c_{ij} = (a_{i1} \otimes a_{1j}) \oplus (a_{i2} \otimes a_{2j}) \oplus \dots \oplus (a_{in} \otimes a_{nj}) < \frac{n}{(2n-1)} = a_{ij}$$

Letting $A^3 = (d_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$,

$$d_{ij} = (c_{i1} \otimes a_{1j}) \oplus (c_{i2} \otimes a_{2j}) \oplus \dots \oplus (c_{in} \otimes a_{nj})$$

From $c_{ik} \otimes a_{kj} < a_{ik} \otimes a_{kj}$ we deduce that

$$d_{ij} = (c_{i1} \otimes a_{1j}) \oplus (c_{i2} \otimes a_{2j}) \oplus \dots \oplus (c_{in} \otimes a_{nj}) < c_{ij}$$

We prove that with $A^n = (a_{ij}^{(n)})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}, (a_{ij}^{(n)})_{n \in \mathbb{N}}$ is a decreasing sequence lower

bounded by 0 thus converging.

Case 2: $(\forall 1 \leq i, j \leq n), a_{ij} \geq \frac{n}{(2n-1)}$; the same reasoning as in case 1 applies only by switching strictly lower than in case 1 with greater than.

Case 3: General case: With $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ and $A^2 = (a_{ij}^{(2)})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$;

if $a_{ij} < a_{ij}^{(2)}$, then $\forall n \geq 1, a_{ij}^{(n)} < a_{ij}^{(n+1)}$.

Prove by induction

$a_{ij}^{(1)} < a_{ij}^{(2)}$ by assumption

Let's suppose that $\forall m < n, a_{ij}^{(m)} < a_{ij}^{(m+1)}$; prove that $a_{ij}^{(n+1)} < a_{ij}^{(n+2)}$

$$a_{ij}^{(n+1)} = (a_{i1}^{(n)} \otimes a_{1j}) \oplus (a_{i2}^{(n)} \otimes a_{2j}) \oplus \dots \oplus (a_{in}^{(n)} \otimes a_{nj})$$

$$a_{ik}^{(n)} \otimes a_{kj} = \max(0, a_{ik}^{(n)} + a_{kj} - 1) < \max(0, a_{ik}^{(n)} + a_{kj}^{(2)} - 1) = a_{ik}^{(n)} \otimes a_{kj}^{(2)}$$

As this is true for all $k = 1, 2, \dots, n$,

$$a_{ij}^{(n+1)} = (a_{i1}^{(n)} \otimes a_{1j}) \oplus (a_{i2}^{(n)} \otimes a_{2j}) \oplus \dots \oplus (a_{in}^{(n)} \otimes a_{nj}) <$$

$$(a_{i1}^{(n)} \otimes a_{1j}^{(2)}) \oplus (a_{i2}^{(n)} \otimes a_{2j}^{(2)}) \oplus \dots \oplus (a_{in}^{(n)} \otimes a_{nj}^{(2)}) = a_{ij}^{(n+2)}$$

Example: Let $A = \begin{bmatrix} 0.8 & 0.4 & 0.5 \\ 0.5 & 0.9 & 0.1 \\ 0.6 & 0.6 & 0.3 \end{bmatrix}; A^7 = A^6 = \begin{bmatrix} 1 & 1 & 0. \\ 1 & 1 & 0. \\ 1 & 1 & 0. \end{bmatrix}$

This computation is obtained using the fuzzy product function below in Exhibit 1.

Exhibit 1: An algorithm for fuzzy product

```
function [C] = fuzzyproduct(B,A)
function [c] = probasum(a,b)
c = a + b - (a * b);
end
if size(A,2) ~ = size(B,1)
    fprintf('\n The product is not possible \n')
    close()
else
    C = zeros(size(A,1),size(B,2));
    D = zeros(size(A,1),size(B,2),size(B,1));
    for i = 1:size(A,1)
        for j = 1:size(B,2)
            for k = 1:size(B,1)
                D(i,j,k) = A(i,k) * B(k,j);
                C(i,j) = probasum(D(i,j,k), C(i,j));
            end
        end
    end
end
end
```

As an example, consider the matrix A derive from a five-node MANET:

$$A = \begin{bmatrix} 1.0000 & 0.3910 & 0 & 0.1114 & 0 \\ 0.3910 & 1.0000 & 0.3910 & 0.5594 & 0.1114 \\ 0 & 0.3910 & 1.0000 & 0.5594 & 0.5594 \\ 0.1114 & 0.5594 & 0.5594 & 1.0000 & 0.3910 \\ 0 & 0.1114 & 0.5594 & 0.3910 & 1.0000 \end{bmatrix}$$

The matrix elements, a_{ij} represent a fuzzy view of the node j from node i. Each entry of the principal diagonal of the connectivity matrix is equal 1 with the assumption that any node is fully viewed from its location. The fuzzy product computation is shown below and it converges to **ones(A)** according to Proposition 1.

$$\begin{aligned} A^2 &= \text{fuzzyproduct}(A, A) = \begin{bmatrix} 1.0000 & 0.3910 & 0 & 0.1114 & 0 \\ 0.3910 & 1.0000 & 0.3910 & 0.5594 & 0.1114 \\ 0 & 0.3910 & 1.0000 & 0.5594 & 0.5594 \\ 0.1114 & 0.5594 & 0.5594 & 1.0000 & 0.3910 \\ 0 & 0.1114 & 0.5594 & 0.3910 & 1.0000 \end{bmatrix}^2 \\ &= \begin{bmatrix} 1.0000 & 0.6522 & 0.2057 & 0.3831 & 0.0852 \\ 0.6522 & 1.0000 & 0.7611 & 0.8613 & 0.5180 \\ 0.2057 & 0.7611 & 1.0000 & 0.8815 & 0.8549 \\ 0.3831 & 0.8613 & 0.8815 & 1.0000 & 0.7611 \\ 0.0852 & 0.5180 & 0.8549 & 0.7611 & 1.0000 \end{bmatrix} \\ A^3 &= \text{fuzzyproduct}(A, \text{ans}) = \begin{bmatrix} 1.0000 & 0.8484 & 0.5572 & 0.7021 & 0.3617 \\ 0.8484 & 1.0000 & 0.9464 & 0.9740 & 0.8369 \\ 0.5572 & 0.9464 & 1.0000 & 0.9805 & 0.9617 \\ 0.7021 & 0.9740 & 0.9805 & 1.0000 & 0.9333 \\ 0.3617 & 0.8369 & 0.9617 & 0.9333 & 1.0000 \end{bmatrix} \\ A^{18} &= \begin{bmatrix} 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \\ 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \\ 0.9999 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \\ 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \\ 0.9999 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \end{bmatrix} \end{aligned}$$

And

$$A^{19} = \begin{bmatrix} 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \\ 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \\ 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \\ 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \\ 1.0000 & 1.0000 & 1.0000 & 1.0000 & 1.0000 \end{bmatrix}$$

Definition 8: A MANET matrix is any square matrix with principal diagonal entry equal 1 and others entries taking value in $[0, 1]$.

Definition 9 (Node connectivity): Given a MANET matrix, a node connectivity is the sum of the associated row and column minus 2, this divided by the network size (number of nodes). That is:

$$conn_i = (\sum_j a_{ij} + \sum_j a_{ji} - 2)/(n - 1)^2 \quad (3)$$

This node connectivity tells the user agent when to initiate a movement to increase its connectivity. This definition has two extreme cases: The full-connected connectivity matrix *ones*(*n*) where the node connectivity of all nodes is equal 1; and the totally disconnected network *eye*(*n*) where all nodes have connectivity 0. Consider the MANET matrix B below, and using definition 9 in equation 3:

$$B = \begin{bmatrix} 1.0000 & 0.6342 & 0 & 0 & 0.0377 & 0 \\ 0.5046 & 1.0000 & 0 & 0 & 0.1459 & 0 \\ 0 & 0 & 1.0000 & 0.3908 & 1.0000 & 0.0068 \\ 0 & 0 & 0.0326 & 1.0000 & 0.4262 & 0.0216 \\ 0.0273 & 0.1329 & 0.0847 & 0.4331 & 1.0000 & 0.0220 \\ 0 & 0 & 0.0263 & 1.0000 & 1.0000 & 1.0000 \end{bmatrix}$$

connectivity of node 1 is 0.022784,
connectivity of node 2 is 0.056704,
connectivity of node 3 is 0.061648,
connectivity of node 4 is 0.092172,
connectivity of node 5 is 0.132392 and
connectivity of node 6 is 0.083068

In a KANA algorithm, we allow free node movements in a MANET structure. Agents can enter and leave a MANET; they could also change their positions in the network. In a matrix form, an agent entering the network will result in a change of dimension of the network. If a MANET has a dimension *n* (*n* agents), a new agent coming in will increase the dimension of the network from *n* to *n + 1*. It means the evolution of the MANET is represented by a new matrix where a new row and a new column has been add; the diagonal is 1 and at least one of the entry of the new adding row or column is different from 0.

3.4. Learning, Predicting, and Adaptation by MANET Nodes

Reasoning from the classical control theory governing dynamic systems, let equation (3) represent the rate of change of the system, is a fuzzy matrix governing the process or dynamic of the network, and x_0 is the initial system state.

$$\dot{X} = AX + BU \quad (3)$$

The matrix $A_{(n \times n)}$ represents a process that describes how an agent *i* influences agent *j* through some interactions, U is an influence vector that describes the intrinsic node characteristic, U has *p* × *n* dimension, with *n* = number of MANET nodes, and *p* = number of intrinsic factors considered. Assuming that each node in the network evaluates each node with respect to each object, we can define a pairwise, non-symmetric, preference *n* × *n* matrix, which defines X.

We can discretize equation 3 to obtain time-dependent values as follows:

$$\begin{aligned} \dot{x} = Ax + b \text{ is } \frac{x_{t+1} - x_t}{\Delta t} &= Ax_t + b \\ \frac{x_{t+1} - x_t}{\Delta t} = Ax_t + b &\Rightarrow x_{t+1} - x_t = \Delta t(Ax_t + b) \\ &\Rightarrow x_{t+1} = x_t + \Delta t(Ax_t + b) \end{aligned} \quad (4)$$

$$\Rightarrow x_{t+1} = (I + \Delta t A)x_t + \Delta t b$$

Let $B_t = I + \Delta t A$ and $b_t = \Delta t b$, $x_{t+1} = B_t x_t + b_t$; x_t is the network configuration at time t , and x_{t+1} is the network configuration at time $t + 1$.

The discrete form is now defined in equation 5.

$$X_{t+1} = A_t X_t + B U \quad (5)$$

From the description of network node behaviors in equation (5), the matrix A represents a process that describes how an agent i influences agent j through some interactions.

From now on, the state of a network with n agents is represented by a $n \times n$ -square matrix with principal diagonal equal 1; an entry in row i and column j represents the relative viewpoint of agent i to agent j . The general MANET state evolution equation of the network in term of fuzzy matrices is given by equation 6

$$X_{t+1} = (A_t \otimes X_t) \oplus B_t \quad (6)$$

Where \otimes is the fuzzy multiplication of fuzzy matrices and \oplus is the fuzzy addition; A_t , and B_t are matrices representing the behavior evolution process at t iteration, and, X_t is a matrix of network configuration (e.g. adjacency matrix) of the network at t iteration.

3.5. Chapter Summary

The chapter discussed a fuzzy-based agent models for modeling MANET behaviors. A fuzzy connectivity matrix is used to represent a MANET. Under the assumption of region of access (ROA) model suggested by Weisstein (<http://mathworld.wolfram.com/Circle-CircleIntersection.html>), each entry into the fuzzy matrix is derived as a disk with radius equal to its energy level. Thus, a MANET with n nodes has a fuzzy matrix in which each row of the matrix is associated to a node of the MANET and the element a_{ij} of the matrix is a fuzzy number representing how a node i “views” node j within the same MANET architecture. An example of a node viewpoint may be in terms of how information is shared with other nodes. We develop an algorithm for calculating the evolutionare behaviors of MANET nodes using fuzzy product operations on the matrix. It is shown that after a “sufficiently large number of iterations”, the fuzzy matrix converges to a “zero-one” matrix. The values of “0” and “1” simply means that two edges of the network with “1” have a crisp connectivity (and hence good communication), and those with “0” means no connectivity at all. This transition from a fuzzy matrix to a defined crisp matrix of either 0 or 1 brings interesting results on convergence properties of MANET nodes. This observation will be applied in the simulation experiments in Chapter 4.

CHAPTER 4

AGENT-BASED MODELING AND SIMULATION OF A COGNITIVE MANET

4.1. Foundation of Sociometrics for A Cognitive MANET

This section develops socio-metrics for MANET performance evaluation. It is assumed that a MANET node is a socio-cognitive-technology system whose entities assume the behaviors of human and technology agents. Using the principles of network connectivity, we identify both intrinsic- and system level extrinsic- factors for the model development. The values of the intrinsic- and extrinsic- variables are generated using known fuzzy models discussed in Chapter 3. We analyze the contributions of the socio-metrics to the overall MANET system performance. At the system level, the socio-metric variables used in this study are trust, cooperation, learning, situation awareness, and information sharing. At the node level, the variables used are adaptation, risk taking behavior, decision making, reputation, and self-awareness. Node characteristics are the independent variables which are intrinsically embedded on the nodes. Other important and relevant socio-behavioral issues consider such metrics as trust (Sun, et al., 2006), information sharing (Luo, Zhang, & Leung, 2000), situation awareness (Ensley, 1997), , reputation Klews & Wreschniok(200), security (Zhou, 1990), vulnerability (Karhima, et al., 2005), competition (Thompson, et al., 2012), and cooperation (Srinivasan, et al., 2003). Social trust may include friendship, honesty, privacy, and social reputation and recommendation derived from direct or indirect interactions for “sociable” purposes (Theodorakopoulous & Baras, 2012). In MANETs, some metrics to measure these social trust properties can be the frequency of communications, malignant or benign behaviors (e.g., false accusation, impersonation), and quality of reputation. Yu *et al.* (2003) used social networks to develop a composite trust value of all the nodes in a social network. Gong, et al. (2009) evaluated the social values of network nodes in terms of the degree of personal or social trends, rather than the capability of executing a mission based on past collaborative interactions. Younis, et al. (2010) reasoned that a proper representation of other socio-metric properties will lead to the design of a cognitive MANET. It is suggested in Thomas, et al.(2005) that we need to include network properties that can measure individual and collective agent behaviors in the network The issue of a selfish behavior is also important in human-machine systems. Selfish nodes in a network are characterized by their reluctance to spend resources, or to cooperate with other nodes.

We consider collaboration to be associated with selfishness as evidenced when a MANET node seeks to conserve battery energy which may lead to less communication with friendly nodes. Thus, as a part of performance, the impact of the nodes’ selfish behaviors on the system performance can be useful in allocating resources and training for collaboration, thereby increasing the collaboration behaviors among the participating nodes in a network.

When subjected to different information loading and traffic scheduling schemes, a MANET can exhibit many emerging behaviors. Although this problem has been addressed from a physical system phenomenon, observing human behaviors (subjective data) and combining them with the physical data from the network can be informative. BARTER (Frias-Martinez, et al., 2007), a behavior-based access control and communication security framework for MANETs reveals that behaviors of the agents (or

nodes) within a network have powerful influence on the system performance. It is noted in BARTER that mutual information and self-information efficacy may be useful in analyzing a system level performance using both physical and behavioral properties.

Currently, models that encourage cooperativeness, collaboration and less competition for resources in MANET nodes using behavioral data are few and nascent. These attributes are beginning to be addressed as factors in performance modeling. For example, Zhang, et al. (20030) developed a model in which each node is responsible for independently conducting localized intrusion detection and with sharing data with neighboring nodes to provide a collaborative detection on a broader level. The intrusion detection agents on the nodes communicate via a secure communication channel with cooperative detection engines

4.2. Some Challenges to Socio-metric Development

There are many challenges and opportunities in developing socio-metrics MANETs. Some of these challenges are:

Resource sharing behaviors: DaSilva and Srivastava (2004) note that voluntary resource sharing in networks has consequences on how network systems recover from attack.

Conflict and cooperation: Considered as rational decision making agents, MANET nodes behave autonomously to preserve their sometimes unchecked behaviors which may have conflicting values with overall system level cooperation (Axelrod, 1984).

Dynamic nature of the users: MANET nodes are highly mobile and with variations in task expectations. A MANET is a peer-to-peer network that consists of a large number of nodes that may be highly mobile; an effective intrusion detection approach cannot rely on the presence of any particular node at any particular point in time (Ragharam, et. al ,2007).

Dimensions of human-machine interface: Tan, Zhou, Ho, Mehta, and Tanabe (2002) observed that an objective evaluation of a system like MANET is difficult to achieve because of the distributed behaviors between humans and devices at the node level, and the interaction of information entropies across node levels.

Reliability: MANET devices, including humans, are prone to failures and stresses. In addition, providing real-time services such as voice or video over ad hoc networks represent a very challenging task in securing machine code intruders or decoding frequency information across some targeted spectra (Venkatraman, et al., 2010). Also, there is typically less network bandwidth available in MANETs than can be provided in the traditional wired networks and wireless local area networks. As a result, information passed between the distributed nodes must be prioritized for transmission against outside attacks. This can be an expensive undertaking and can bias the opinions of individual nodes (with the humans) regarding the perception of each other.

Lack of a centralized control: The nodes in a MANET are distributed independent entities reliant on localized connectivity. Hence, there is no single node that is designed to act as a controller hub for other components in the MANET. As a result, there is similarly no possibility for a centralized detection monitor that can coordinate the inputs from host-based intrusion detections on each node.

Learning: Given that the configuration of a MANET has a role in the formation of opinions and beliefs, and the subsequent shaping of behaviors, it is important that we analyze how the structure of a MANET affects learning and the diffusion of information.

Trust: Literature has identified a large variety of factors and mechanisms that contribute to the dynamics of trust in a MANET, ranging from node attributes, characteristics of the work environment and the MANET design elements. Although the trust literature seems to be differentiated, researchers across disciplines agree that trust is an interpersonal (i.e. dyadic) concept. Within the network tradition, trust is explicitly conceptualized as an interpersonal relationship, which in general is embedded in triadic and even more complex configurations of relations (Burt, 1992). Furthermore, network research on trust has also shown that it affects organizational performance and intra-organizational dynamics.

4.3. Modeling Socio-behavioral Metrics in a MANET

As discussed before, a MANET system has intrinsic (i.e., peculiar to itself)-and extrinsic (related with other) nodes – properties (Figure 7). Some examples of extrinsic social properties of MANETs are results of interactions among nodes and they represent system level measures of performance. Some examples are trust, cooperation, situation awareness, and the ability to share information.

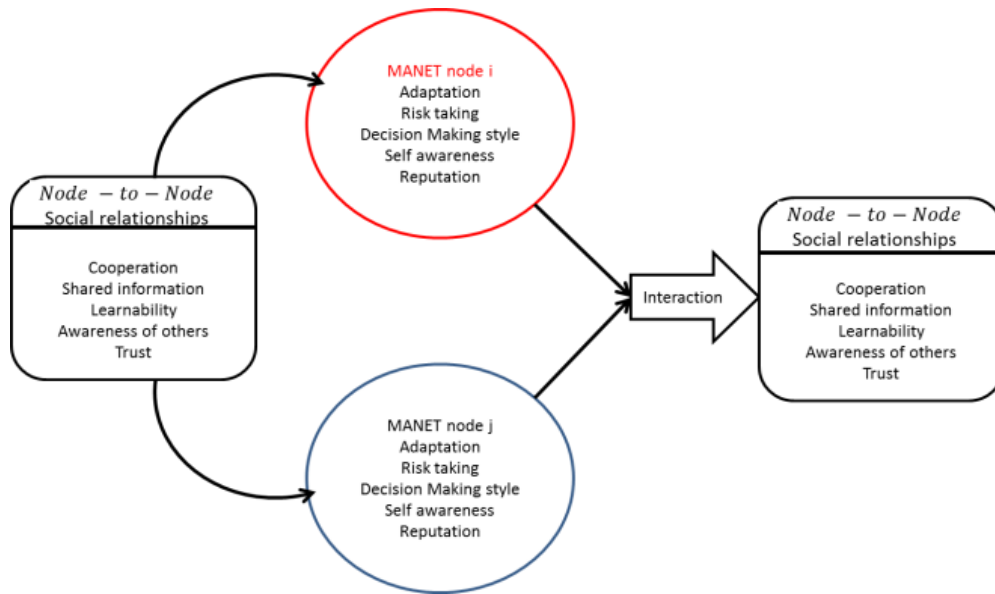


Figure. 7. Sample socio-cognitive properties of MANET nodes.

Consider a MANET with ten nodes with five intrinsic nodal properties with values calibrated on a scale of 0 to 1 (based on subjective past performance as rated by experts). The intrinsic properties of each node are rated on, for example, the ability to adapt (Adaptation); the ability to take risks (Risk-taking); decision making; awareness of surroundings (Self-awareness); and Reputation. An example data for node 1 is shown by the vector denoted by \mathbf{Z} , a vector of $p \times 1$ in dimension, with p representing the number of node intrinsic properties. When all the data in \mathbf{Z} vector are concatenated over all nodes,

we have $p \times n$ matrix, $Z_{p \times n}$, with n representing the number of nodes in a MANET.

$$Z = \begin{bmatrix} \text{Adaptation} \\ \text{Risk - Taking} \\ \text{Decision - Making} \\ \text{Self - Awareness} \\ \text{Reputation} \end{bmatrix} = \begin{bmatrix} 0.77 \\ 0.69 \\ 0.47 \\ 0.87 \\ 0.58 \end{bmatrix}$$

With these intrinsic properties we can calculate the inter-node similarity between nodes by equation 7a

$$\text{sim}(Z_1, Z_2) = 1 - d(Z_1, Z_2) \quad (7a)$$

$$\text{Where } d(Z_1, Z_2) = \left[\frac{\sum_{i=1}^p (\mu_{Z_1}(x_i) - \mu_{Z_2}(x_i))^2}{p} \right]^{1/2} \quad (1b) \quad (7b)$$

Where $\mu_z(z)$ represents the fuzzy value of an intrinsic property;

$d(Z_1, Z_2)$ Satisfy the properties:

$$d(Z_1, Z_2) = 0 \Leftrightarrow Z_1 = Z_2,$$

$$d(Z_1, Z_2) + d(Z_2, Z_3) \geq d(Z_1, Z_3), \text{ and}$$

$$d(X_2, X_1) = d(X_1, X_2)$$

$$\text{As an example, Let } Z_1 = \begin{bmatrix} 0.77 \\ 0.69 \\ 0.47 \\ 0.87 \\ 0.58 \end{bmatrix}; Z_2 = \begin{bmatrix} 1.0 \\ 0.3 \\ 0.7 \\ 0.78 \\ 0.85 \end{bmatrix};$$

$\mu_{Z_1}(\text{Adaptation}) = 0.77$, $\mu_{Z_1}(\text{Risk - Taking}) = 0.69$, $\mu_{Z_1}(\text{Decision - Making}) = 0.47$,
 $\mu_{Z_1}(\text{Self - Awareness}) = 0.87$ and $\mu_{Z_1}(\text{Reputation}) = 0.58$. Similarly for μ_{Z_2} , the values are given in a vector form above. Then, $d(Z_1, Z_2)$ is calculated by equation (1b) as:

$$\begin{aligned} &= \left[\frac{(0.77 - 1)^2 + (0.69 - 0.3)^2 + (0.47 - 0.7)^2 + (0.87 - 0.78)^2 + (0.58 - 0.85)^2}{5} \right]^{1/2} \\ &= 0.2424, \\ \text{sim}(Z_1, Z_2) &= 1 - d(Z_1, Z_2) = 0.7576. \end{aligned}$$

We are interested in calculating a system level performance using intrinsic factors as independent variables. The system level performance attributes selected for demonstration analysis are trust, information sharing, cooperation, and situation awareness of each other. The original ground truth data on each of the system performance measures is obtained by asking the human experts of node i to rate node j , and vice versa, with a node self-rating defaulting to a unity. Equivalently, it can be obtained by some closed form fuzzy models such as described in Mathworld. The models used to generate the extrinsic scores are described below in section 4.2.

4.4. Socio-metric Properties of a MANET

Consider the inter-rater assessment matrix of $n \times n$ dimension in which each MANET node (agent) i rates agent j on the system level measures. The pair-wise matrices are non-symmetric since each agent has a different concept or opinion of

another agent. At each epoch in which a node is engaged in some activity, the intrinsic properties are assumed to change based on new information and interactions. During any iteration, the node characteristics (intrinsic properties) are updated. This updating behavior is governed by equation 8

$$Z_k = X_{k-1} \otimes Z_k \quad (8)$$

Where, Z_k is a vector of the intrinsic properties (discussed earlier) at time k ; X_k is the fuzzy connectivity matrix at time k , and \otimes is the fuzzy product operator. At each iteration we update the agent characteristics by performing a nonmetric multidimensional scaling on the n -by- n similarity matrix as follows:

$$\text{sim}(Z_1, Z_2) = 1 - d(Z_1, Z_2), \text{ as in equation 7a}$$

$$\text{Trust}_{k+1} = \min(\text{sim}_k, X_k) \quad (9)$$

$$\text{Cooperation}_{k+1} = \text{Trust}_{k+1} \oplus (\text{Cooperation}_k \ominus (1 - \text{Sim}_k)) \quad (10)$$

$$\text{Awareness}_{k+1} = (1 - \text{Trust}_{k+1}) \oplus (\text{Awareness}_k \ominus \text{Sim}_k) \quad (11)$$

$$\text{Information Sharing}_{k+1} = \text{Information Sharing}_k \otimes X_k \quad (12)$$

\oplus and \ominus are the fuzzy addition and subtraction operators (Vasanth, et al., 2007), respectively. In equation 9, we assume that trust scores between two nodes are simply the minimum similarity between the two nodes and their fuzzy connectivity. In equation 10, the cooperation score at $k + 1$ iteration is the fuzzy sum of the trust scores and the cooperation scores at the previous iteration residuated by the negation of their similarity. In equation 11, a node awareness of other nodes in a MANET is the negation of cooperation in the sense that it is the fuzzy sum of mistrust and the awareness at the previous iteration residuated with the similarity. Note that a residuum is simply a part of the extrinsic variables attributed to the other nodes from the primary (i.e., own) node. Morgan and Dilworth (1939) define a residuum of a t-norm operation \oplus and \ominus as universal operations satisfying: $a \oplus b \leq c \Leftrightarrow a \leq c \ominus b$. In equation 12, information sharing is measured as the frequency of communication transactions. The general procedure to implement these network socio-metric behaviors is shown in Exhibit 2.

Generate the initial network G
 Compute the fuzzy connectivity matrix X
 Randomly generate the initial node intrinsic properties Z_1, Z_2, Z_3, \dots
 Randomly generate the initial node extrinsic properties Y_1, Y_2, Y_3, \dots
 $k = 0$
 $G1 = [n_0]$ #Assign information to a randomly generated node
 While $k < n$ and $G1$ is not isomorphic to G : Do
 Generate the MANET evolution processes (A, B)

$$X = (A \otimes X) \oplus B;$$

Update node intrinsic properties

$$\left. \begin{aligned} Z_1 &= X \otimes Z_1 \\ Z_2 &= X \otimes Z_2 \\ Z_3 &= X \otimes Z_3 \\ &\vdots \\ Z_n &= X \otimes Z_n \end{aligned} \right\} \quad \text{Equation 8}$$

Update node extrinsic properties

$$\text{Trust}_{k+1} = \min(\text{sim}_k, X_k) \quad \text{Equation (9)}$$

$$\text{Cooperation}_{k+1} = \text{Trust}_{k+1} \oplus (\text{Cooperation}_k \ominus (1 - \text{Sim}_k)) \quad \text{Equation (10)}$$

$$\text{Awareness}_{k+1} = (1 - \text{Trust}_{k+1}) \oplus (\text{Awareness}_k \ominus \text{Sim}_k) \quad \text{Equation (11)}$$

```

InformationSharingk+1 = InformationSharingk ⊗ Xk Equation (12)
// Update network information before checking the next node in the network.
Let N0 ⊆ N; a set of node already in the network
∀ n ∈ N & n ∉ C
    If sim(n, N0) ≥ α // α is a simulation converging factor & α = 0.5 was chosen based on
    trial run data analysis.
        conn(n, N0) ≥ α, then // conn (n, N0) = X//
        N0 ← N0 ∪ {n}
    Endif
k = k + 1
End while

```

Exhibit 2. An Algorithm for computing MANET socio-metrics

4.5. Simulation Experiments

4.5.1. Input Data

To start the simulation experiment, the user defines the number of nodes in the MANET (in this example, $n = 10$). Next, the intrinsic node values are generated. For our illustration, we use the following: adaptation, risk-taking, decision making, self-awareness and reputation. The initial values of these characteristics are randomly generated from a fuzzy distribution, such that for any node i , its characteristic $x_i \in [0, 1]$. Table 2 shows sample inputs for a ten-node MANET (labeled as agents). As shown in Table 2, node (agent) 1 is not adaptive as its rated value is about 1%, while agent 2 shows a high adaptive rating with 97% value.

The next inputs are the extrinsic socio-metric values. We use cooperation, trust, self-awareness, and information sharing, respectively. Note that many other factors can be added as desired. The extrinsic input is defined as a relative pair-wise and non-symmetric matrix. For each characteristic, there are $n \times n$ relative matrices A such that $A_k \in [0, 1]$ and the values are generated from a fuzzy distribution. Tables 3 to 5 are examples input matrices for cooperation, trust, situation awareness, and information sharing, respectively. In Table 2, for example, nodes 5 and 6 have poor cooperation as their rated value is 11%. Nodes 2 and 9 have a rated value of 92% that shows the possibility of high cooperation between the nodes. The same explanation holds for other matrices in Tables 3 – 4, respectively.

Table 2. Sample node intrinsic characteristic

	A 1	A 2	A 3	A 4	A 5	A 6	A 7	A 8	A 9	A10
Ad	0.01	0.97	0.15	0.28	0.31	0.32	0.23	0.09	1.00	0.87
RT	0.10	0.88	0.42	0.80	0.73	0.47	0.87	0.80	0.32	0.43
DM	0.62	0.83	0.54	0.80	0.53	0.39	0.13	0.71	0.05	0.17
SA	0.39	0.14	0.09	0.45	0.85	0.72	0.30	0.21	0.19	0.79
RP	0.64	0.14	0.85	0.24	0.20	0.48	0.28	0.85	0.52	0.04

Table 3. Sample initial relative rating matrix for cooperation

Coop	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	1	0.07	0.86	0.84	0.56	0.19	0.87	0.22	0.31	0.83
A2	0.82	1.00	0.50	0.72	0.85	0.09	0.29	0.43	0.92	0.38
A3	0.57	0.41	1.00	0.10	0.40	0.05	0.94	0.20	0.25	0.19
A4	0.39	0.79	0.21	1.00	0.75	0.05	0.76	0.32	0.39	0.28
A5	0.42	0.11	0.43	0.48	1.00	0.63	0.86	0.61	0.12	0.31
A6	0.28	0.96	0.88	0.39	0.11	1.00	0.25	0.65	0.88	0.12
A7	0.79	0.65	0.43	0.93	0.56	0.29	1.00	0.59	0.21	0.06
A8	0.49	0.53	1.00	0.61	0.35	0.12	0.66	1.00	0.19	0.30
A9	0.78	0.25	0.29	0.12	0.47	0.24	0.14	0.39	1.00	0.75
A10	0.79	0.14	0.93	0.25	0.47	0.29	0.61	0.26	0.69	1.00

Table 4. Sample initial relative rating matrix for trust

Trust	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	1.00	0.31	0.23	0.03	1.00	0.06	0.57	0.09	0.09	0.67
A2	0.04	1.00	0.40	0.61	0.45	0.52	0.53	0.48	0.99	0.06
A3	0.81	0.25	1.00	0.14	0.87	0.04	0.18	0.88	0.84	0.25
A4	0.67	0.45	0.22	1.00	0.32	0.40	0.96	0.40	0.03	0.11
A5	0.92	0.75	0.48	0.52	1.00	0.75	0.25	0.94	0.47	0.09
A6	0.99	0.16	0.07	0.71	0.82	1.00	0.99	1.00	0.01	0.07
A7	0.81	0.26	0.06	0.59	0.58	0.29	1.00	0.18	0.21	0.59
A8	0.96	0.72	0.03	0.68	0.84	0.65	0.98	1.00	0.48	0.93
A9	0.73	0.99	0.80	0.95	0.94	0.02	0.11	0.11	1.00	0.23
A10	0.05	0.14	0.20	0.29	0.66	0.72	0.42	0.24	0.28	1.00

Table 5. Sample initial relative rating matrix for self-awareness

Aware	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	1.00	0.57	0.34	0.08	0.48	0.82	0.99	0.67	0.43	0.25
A2	0.68	1.00	0.07	0.50	0.48	0.59	0.45	0.79	0.53	0.52
A3	0.20	0.87	1.00	0.13	0.78	0.48	0.82	0.42	0.20	0.76
A4	0.67	0.59	0.50	1.00	0.01	0.51	0.86	0.03	0.06	0.56
A5	0.65	0.74	0.06	0.73	1.00	0.65	0.85	0.36	0.33	0.11
A6	0.22	0.50	0.74	0.53	0.17	1.00	0.20	0.11	0.97	0.68
A7	0.66	0.38	0.91	0.19	0.66	0.94	1.00	0.89	0.40	0.31
A8	0.32	0.16	0.38	0.89	0.31	0.07	0.91	1.00	0.39	0.11
A9	0.41	0.70	0.08	0.37	0.19	0.82	0.16	0.82	1.00	0.59
A10	0.14	0.94	0.08	0.82	0.84	0.78	0.12	0.50	0.89	1.00

Table 6. Sample initial relative rating matrix for information sharing

IS	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	1.00	0.37	0.99	0.08	0.96	0.61	0.55	0.75	0.38	0.68
A2	0.43	1.00	0.96	0.87	0.13	0.11	0.49	0.63	0.09	0.96
A3	0.61	0.12	1.00	0.15	1.00	0.82	0.60	0.93	0.54	0.56
A4	0.54	0.53	0.57	1.00	0.89	0.74	0.39	0.59	0.44	0.63

A5	0.98	0.44	0.39	0.38	1.00	0.98	0.99	0.63	0.42	0.92
A6	0.09	0.41	0.66	0.26	0.53	1.00	0.08	0.34	0.64	0.10
A7	0.96	0.51	0.35	0.52	0.08	0.14	1.00	0.96	0.04	0.20
A8	0.34	0.58	0.80	0.86	0.72	0.67	0.89	1.00	0.29	0.40
A9	0.89	0.75	0.62	0.90	0.05	0.07	0.81	0.20	1.00	0.16
A10	0.33	0.10	0.06	0.75	0.19	0.81	0.81	0.46	0.08	1.00

4.5.2. Simulation Results

The results for the simulation experiments are shown in the displays with the label beginning with the iteration number. Only the first and the last two iterations (8 and 9) are shown here since the solutions almost converge to stable values as shown in Proposition 1 of Chapter 3.

In iteration 1, the simulated system level socio-metrics are: Cooperation: 30.3%; Trust: 17.3%; Situation Awareness: 14.5%; and Information Sharing: 20.7%, respectively. The “Agent” label on the bar chart to the left indicates a MANET node. Nodes 5, 6, and 9 show some level of connectivity (right side of Figure 8) while other nodes operate autonomously as shown at the right hand of the connectivity display. As the simulation progressed, we observed learning taking place resulting in more connectivity as shown in iteration 9. The simulation terminates as soon as the set limit of connectivity is achieved or the final extrinsic output connectivity values are relatively stable, that is, their differences are close the set difference threshold of 0.09. Figure 9 show the results of the last iteration when the simulation converges (See table 8).

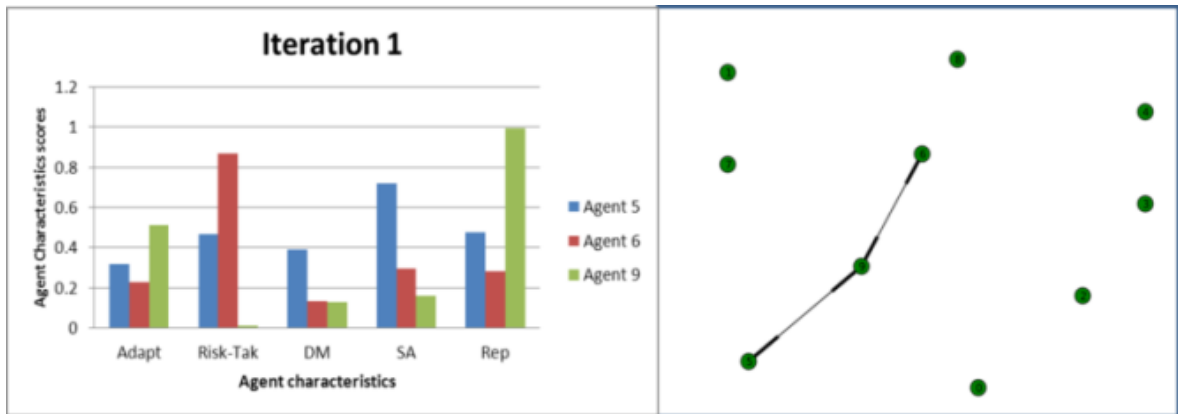


Figure 8. Network physical configuration and graph of agent characteristics at iteration 1

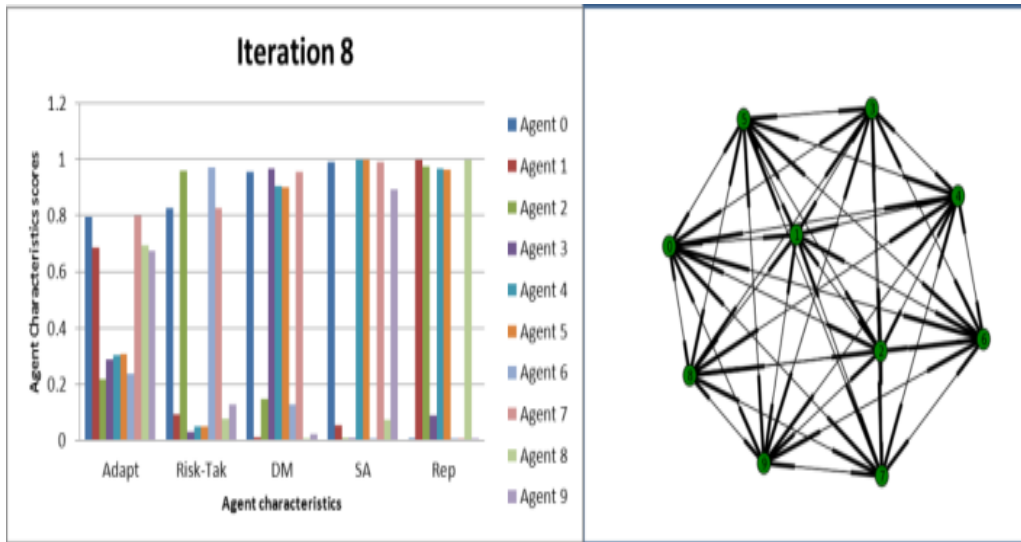


Figure 9 . Network physical configuration and graph of agent characteristics at iteration 8

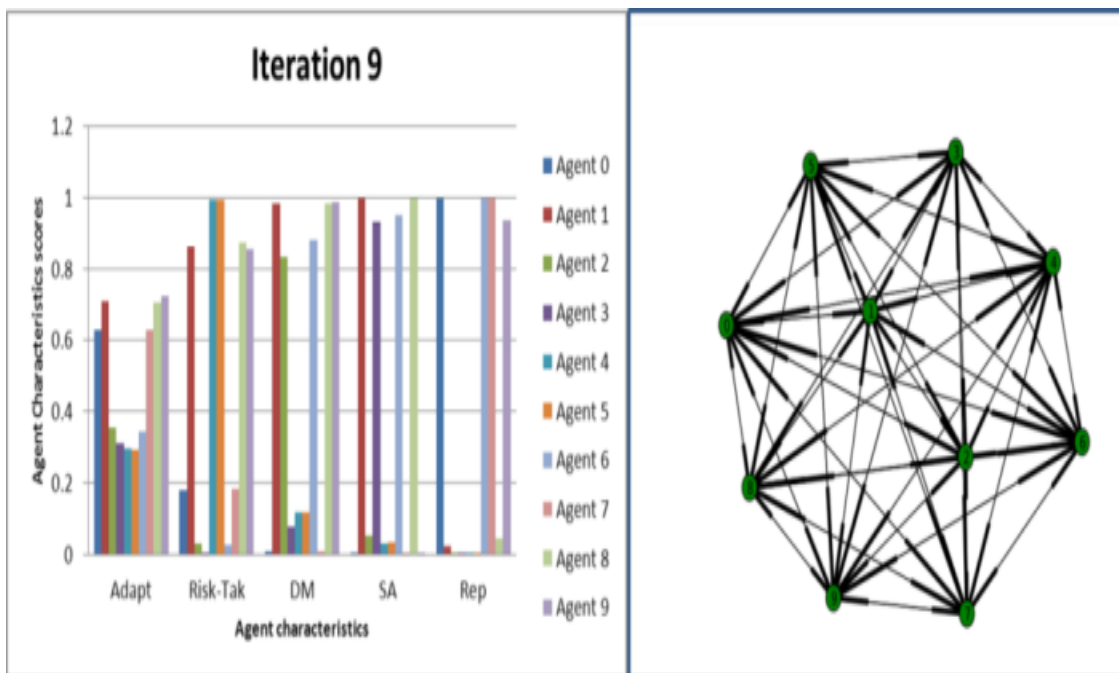


Figure. 10. Network physical configuration and graph of agent characteristics at iteration 8

Table 8. Converging values at the last iteration for cooperation metric.

Coop	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	0.75	0.72	0.75	0.70	0.75	0.70	0.75	0.75	0.75	0.75
A2	0.71	0.71	0.70	0.70	0.71	0.70	0.71	0.71	0.70	0.71
A3	0.71	0.71	0.70	0.70	0.71	0.70	0.71	0.71	0.70	0.71
A4	0.80	0.72	0.70	0.70	0.80	0.70	0.80	0.80	0.70	0.80
A5	0.71	0.71	0.70	0.70	0.71	0.70	0.71	0.71	0.70	0.71
A6	0.75	0.72	0.70	0.70	0.75	0.70	0.75	0.75	0.70	0.75
A7	0.80	0.72	0.70	0.70	0.80	0.70	0.80	0.80	0.70	0.80
A8	0.76	0.72	0.75	0.70	0.76	0.70	0.76	0.76	0.75	0.76
A9	0.80	0.72	0.70	0.70	0.80	0.70	0.80	0.80	0.70	0.80
A10	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70
Trust	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	0.68	0.70	0.75	0.66	0.68	0.70	0.75	0.75	0.70	0.68
A2	0.68	0.70	0.71	0.66	0.68	0.70	0.70	0.71	0.70	0.68
A3	0.68	0.70	0.71	0.66	0.68	0.70	0.70	0.71	0.70	0.68
A4	0.68	0.70	0.80	0.66	0.68	0.70	0.70	0.80	0.70	0.68
A5	0.68	0.70	0.71	0.66	0.68	0.70	0.70	0.71	0.70	0.68
A6	0.68	0.70	0.75	0.66	0.68	0.70	0.70	0.75	0.70	0.68
A7	0.68	0.70	0.80	0.66	0.68	0.70	0.70	0.80	0.70	0.68
A8	0.68	0.70	0.76	0.66	0.68	0.70	0.75	0.76	0.70	0.68
A9	0.68	0.70	0.80	0.66	0.68	0.70	0.70	0.80	0.70	0.68
A10	0.68	0.70	0.70	0.66	0.68	0.70	0.70	0.70	0.70	0.68
Self-Awareness	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	0.66	0.75	0.75	0.75	0.75	0.70	0.75	0.75	0.70	0.75
A2	0.66	0.70	0.70	0.71	0.70	0.70	0.71	0.71	0.70	0.70
A3	0.66	0.70	0.70	0.71	0.70	0.70	0.71	0.71	0.70	0.70
A4	0.66	0.70	0.70	0.80	0.70	0.70	0.80	0.80	0.70	0.70
A5	0.66	0.70	0.70	0.71	0.70	0.70	0.71	0.71	0.70	0.70
A6	0.66	0.70	0.70	0.75	0.70	0.70	0.75	0.75	0.70	0.70
A7	0.66	0.70	0.70	0.80	0.70	0.70	0.80	0.80	0.70	0.70
A8	0.66	0.75	0.75	0.76	0.75	0.70	0.76	0.76	0.70	0.75
A9	0.66	0.70	0.70	0.80	0.70	0.70	0.80	0.80	0.70	0.70
A10	0.66	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70	0.70
Info Sharing	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	0.68	0.60	0.75	0.75	0.75	0.75	0.75	0.75	0.64	0.68
A2	0.68	0.60	0.71	0.71	0.71	0.70	0.71	0.71	0.64	0.68
A3	0.68	0.60	0.71	0.71	0.71	0.70	0.71	0.71	0.64	0.68
A4	0.68	0.60	0.80	0.80	0.72	0.70	0.80	0.80	0.64	0.68
A5	0.68	0.60	0.71	0.71	0.71	0.70	0.71	0.71	0.64	0.68
A6	0.68	0.60	0.75	0.75	0.72	0.70	0.75	0.75	0.64	0.68
A7	0.68	0.60	0.80	0.80	0.72	0.70	0.80	0.80	0.64	0.68
A8	0.68	0.60	0.76	0.76	0.75	0.75	0.76	0.76	0.64	0.68
A9	0.68	0.60	0.80	0.80	0.72	0.70	0.80	0.80	0.64	0.68
A10	0.68	0.60	0.70	0.70	0.70	0.70	0.70	0.70	0.64	0.68

Table 9 gives the summary of the system level values based on the operations on all the input matrices. Note that the outputs of the socio-metrics are scaled to add to 100% over

the set of selected extrinsic, system-level variables assessed. This is done in order to associate the performance of the variables to a common metric.

Table 9. A summary of socio-metrics derived from node connectivity simulation (%)

Simulation iteration #	Cooperati- on	Trust	Self Awareness	Information Sharing
1	33.85	10.74	30.89	24.52
8	24.98	24.90	25.06	25.06
9	24.13	24.13	26.89	24.85

Other information on the simulation results are shown in Appendix A of this report.

4.6. Chapter Summary

As shown in Table 9, the initial system level characteristics after iteration 1 were, 33.85% of Cooperation, 10.74% for Trust, 30.89% for Self-awareness, and 24.52% for Information Sharing. In the first iteration, it can be seen that the system trust value of 10% is very low when compared to other variables. As the nodes in the network learned to know each other, the metrics tended to increase connectivity with other nodes, and thus, the Trust value increased from 10.74 to 24.13% (almost 125% increase). The decrease in values for Cooperation (from 33.85 % to 24.13%) and Self-awareness (from 30.89% to 26.89%) does not mean that there was a decrease in how the nodes cooperated or had self-awareness. It simply means that nodes with high cooperation and self-awareness were likely to share information and created more trust in the network as time evolved. This was achieved by incorporating behavior updating mechanisms into the simulation model. The learning mechanism systematically trains nodes in the MANET system to cooperate, trust, share information, and have self-awareness by adjusting their individual achievement weights (sociometric scores). In terms of design, it means that a MANET system should be designed with carefully chosen degrees of importance or weights so as to allow better node-to-node connectivity.

CHAPTER 5

SENSITIVITY ANALYSES OF A MANET AGENT'S USE OF SOCIOMETRIC FOR LEARNING AND ADAPTATION

5.1 Background

Learning is important for MANET simulation for many reasons. For example, a lack of trust will result in denying friendly agents of important information and may reduce the level of cooperation between nodes. A node may also learn to be selfish because of a degraded system leading to reduced energy. It can also provide information on what contributes to selfish behaviors of MANET nodes. As noted by Djenouri and Badache (2008), selfish behavior can arise simply by an attempt of a MANET to preserve its own battery. In this case, a node may behave selfishly and would not forward packets originated from other nodes, while using their services and consuming their resources. This deviation from the correct behavior represents a potential threat against the quality and the availability of the forwarding service. With this observation, it is important that the agents learn to cope with degraded operating environments. Our approach is to provide a framework for analyzing models that impact collaborating agents who are likely to share their experiences with each other from sociometric data as well as being cognizant of its individual coping behaviors within the context of operations.

To motivate learning by MANET agents, Djenouri and Badache (2008) have demonstrated, using simple domains, that it is possible to overcome communication barriers by equipping agents with imitation-like learning behaviors. Using imitation, agents can learn from others without communicating an explicit context for the applicability of a behavior. This approach can be used to empower MANET agents with human-like learning strategies.

In machine learning literature (Mitchell, 1997), there are two main types of learning. The first is unsupervised learning, which groups objects into classes based on similarities between them. The second approach is the supervised learning, which is based on a training set consisting of objects whose class is known a priori. In this type of learning, a teacher (or supervisor, hence the name of supervised learning) provides either the action that should be performed, or a gradient of the error. In both cases, the master controller provides an indication of the action that is expected to generate in order to improve its performance. The use of such an approach presupposes the existence of an expert to provide a set of examples, called case-based learning, training situations and correct actions associated. These examples should be representative of the task.

One variant of a supervised learning is reinforcement learning (RL). RL algorithm is the best suited to solving the problems addressed in this project. The unsupervised learning, also called learning from observations is used to determine a classification from a set of objects or situations. It has a mass of undifferentiated data, and we want to know if they have any group structure. It is a question of identifying a possible trend data to be grouped into classes. This type of learning is known as clustering and is found in the automatic classification of information. A typical clustering algorithm searches for patterns among a set of examples, not necessarily guided by the use made of the knowledge learned. It includes all the examples so that the examples within the same group are similar enough, and examples of different groups are sufficiently different.

RL is a variant of supervised learning (Kaelbling, Littman and Moore, 1998). In contrast to the supervised approach, the master in reinforcement learning has a role of evaluator, not an instructor which is usually called critics. The role of the critic is to provide a measure indicating whether the generated action is appropriate or not. This is an agent program through an assessment of penalty or reward without the need to specify how the task should be completed. In this context, we must tell the system what is the goal, and one must learn through a series of trials and errors (in interaction with the environment) how to achieve the goal.

Components of reinforcement learning are the "apprentice" agents, the environment and the task the agent must perform. The interaction between the agent and the environment is continuous. On one hand, the decision-making process of the agent chooses actions according to situations perceived from the environment, and secondly these situations evolve under the influence of these actions. Whenever the agent performs an action, it receives a reward. This is a scalar value indicating to the agent the value of this action. The goal for the agent is to maximize the sum of received reinforcements, and learning takes place in many experiments.

5.2 Learning by MANET Agents

In this research, we adopt the definition of learnability by an agent as the rate of change of its sociometric characteristics with respect to the rate of change of others agent's characteristics viewing as its environment. We characterized learning in terms of how each agent accommodates the change in its environment. Learnability parameter is defined by:

$$L_t^i = \frac{\frac{\text{norm}(X_{t+1}^i)}{\sum_{i=1}^n \text{norm}(X_{t+1}^i)} - \frac{\text{norm}(X_t^i)}{\sum_{i=1}^n \text{norm}(X_t^i)}}{\frac{\text{norm}(X_t^i)}{\sum_{i=1}^n \text{norm}(X_t^i)}} \quad t > 1 \quad (13)$$

Where, $L_0^i = 0 \ \forall i$, and the following interpretation of L_t^i .

$$\begin{cases} L_t^i > 0, & \text{agent perceives an increase in sociometric values} \\ L_t^i = 0 & \text{no change in sociometric value} \\ L_t^i < 0 & \text{agent perceives a reduction in sociometric values} \end{cases}$$

X_t^i is agent i extrinsic characteristics at iteration t and $\text{norm}(X)$ the norm of a vector X is defined as

$$\text{norm}(X) = \text{fuzzydistance}(0, X)$$

Tables 10 and 11 are used to illustrate examples for calculating learnability index with simulated cooperation data.

Table 10. Cooperation scores at iteration 1

Cooperation	0.79	0.79	0.69	0.72	0.79	0.69	0.48	0.65	0.79	0.38
	0.64	0.64	0.61	0.64	0.56	0.33	0.64	0.61	0.36	0.36
	0.68	0.46	0.68	0.46	0.47	0.40	0.61	0.43	0.68	0.68
	0.66	0.65	0.54	0.66	0.56	0.29	0.66	0.59	0.54	0.54
	0.50	0.65	0.65	0.48	0.64	0.65	0.64	0.65	0.65	0.50
	0.56	0.83	0.83	0.51	0.47	0.83	0.56	0.65	0.83	0.56
	0.54	0.50	0.54	0.54	0.68	0.63	0.68	0.61	0.50	0.54
	0.57	0.41	0.79	0.34	0.45	0.34	0.79	0.34	0.45	0.45
	0.42	0.53	0.53	0.43	0.43	0.53	0.43	0.53	0.53	0.33
	0.60	0.60	0.80	0.61	0.60	0.38	0.66	0.80	0.60	0.38

Table 11. Cooperation scores at iteration 2

Cooperation	0.64	0.70	0.70	0.64	0.56	0.70	0.64	0.65	0.70	0.56
	0.68	0.65	0.71	0.66	0.56	0.49	0.71	0.59	0.68	0.68
	0.50	0.51	0.51	0.48	0.51	0.51	0.51	0.51	0.51	0.50
	0.60	0.60	0.73	0.61	0.60	0.53	0.70	0.73	0.60	0.49
	0.57	0.65	0.77	0.53	0.64	0.65	0.77	0.65	0.65	0.53
	0.68	0.65	0.68	0.64	0.68	0.65	0.68	0.65	0.68	0.68
	0.66	0.67	0.80	0.66	0.68	0.67	0.68	0.80	0.67	0.56
	0.68	0.60	0.76	0.61	0.60	0.53	0.72	0.76	0.68	0.68
	0.66	0.65	0.68	0.66	0.64	0.65	0.68	0.65	0.65	0.54
	0.66	0.65	0.57	0.66	0.56	0.57	0.66	0.59	0.57	0.56

X_1^1 is the first row vector of Table 10

0.79	0.79	0.69	0.72	0.79	0.69	0.48	0.65	0.79	0.38
------	------	------	------	------	------	------	------	------	------

$$\text{norm}(X_1^1) = \text{fuzzydistance}(0, X_1^1)$$

$$= \sqrt{\frac{0.79^2 + 0.79^2 + 0.69^2 + 0.72^2 + 0.79^2 + 0.69^2 + 0.48^2 + 0.65^2 + 0.79^2 + 0.38^2}{10}}$$

$$= 0.2929$$

X_2^1 is the first row vector of Table 11

0.64	0.70	0.70	0.64	0.56	0.70	0.64	0.65	0.70	0.56
------	------	------	------	------	------	------	------	------	------

Similarly,

$$\text{norm}(X_2^1) = 0.2097$$

$$L_2^1 = \frac{\frac{0.2097}{\sum_{i=1}^n \text{norm}(X_{t+1}^i)} - \frac{0.2929}{\sum_{i=1}^n \text{norm}(X_t^i)}}{\frac{0.2929}{\sum_{i=1}^n \text{norm}(X_t^i)}} = -0.39$$

$L_2^1 = -0.39$ means that there is a likely reduction in how agent 1 cooperates with other agents.

Figure 11 shows the learning profile for all agents in a cooperation case. Note that in iteration 2, the decreasing average learning cooperation value indicates the possible initial lack of interaction across agents. Figure 12 shows the bar graph of each agent learning to cooperate during a simulation. The groupings of how cooperation evolves between the interactions are shown in Figure 13. From Figure 12 and 13, agents 1, 9 and 10 had the most obvious tendencies to reduce cooperation with others agents.

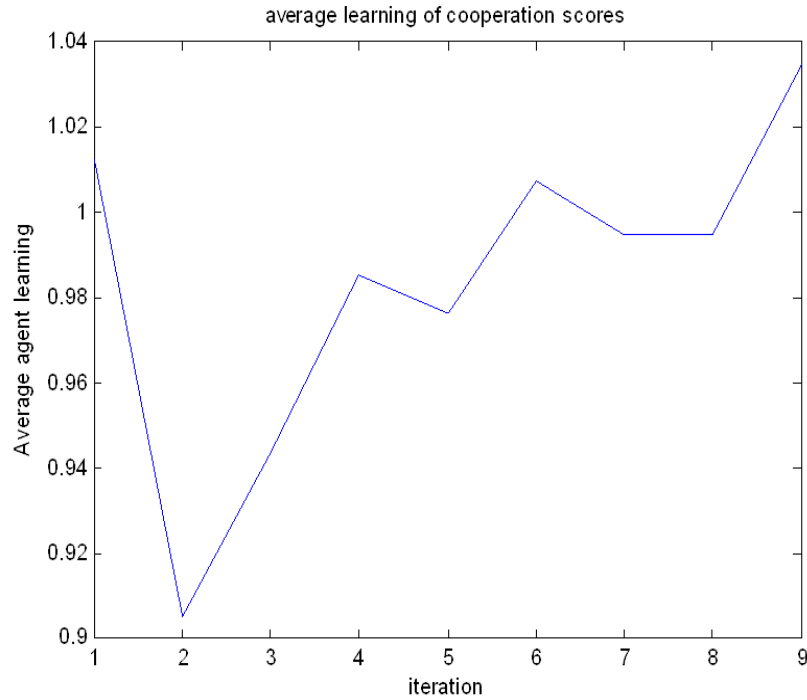


Figure 11. Evolution of average learning factor on cooperation scores.



Figure 12. Average learning factor on cooperation scores for each agent.

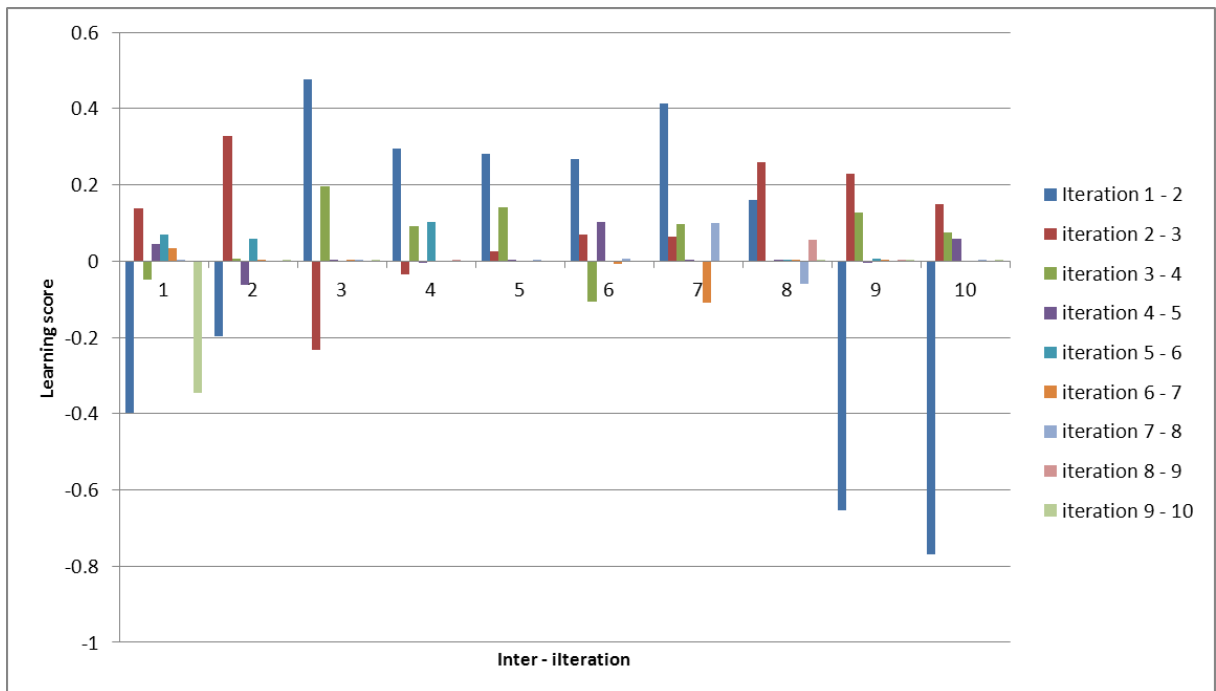


Figure 11. Learning factor on cooperation scores for each agent.

Figure 14 shows the learning profile for all agents in trust score. Note that in iteration 2 as for cooperation score, the decreasing average trust learning indicates the possible initial lack of interaction across agents. Figure 15 shows the bar graph of each agent trust learning during the simulation. The groupings of how cooperation evolves between the interactions are shown in Figure 16. From Figure 15 and 16, agents 1, 8, and 10 had the most obvious tendencies to reduce trust with others agents.

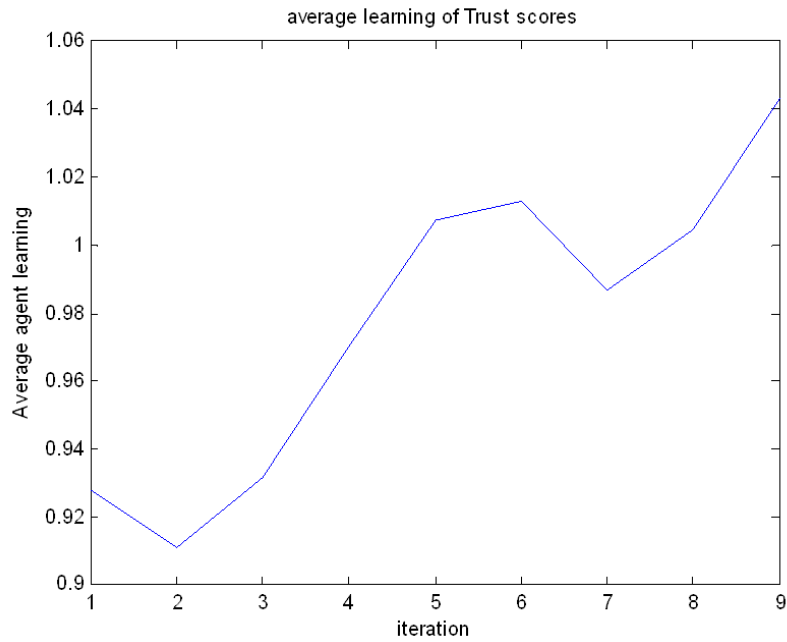


Figure 14. Evolution of average learning factor on trust scores.

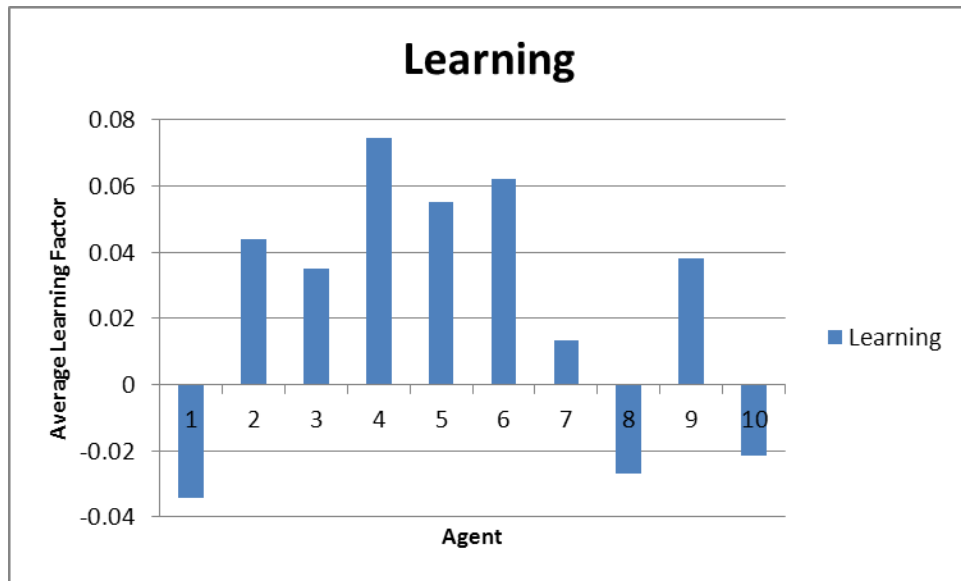


Figure 15.. Learning factor on trust scores for each agent.

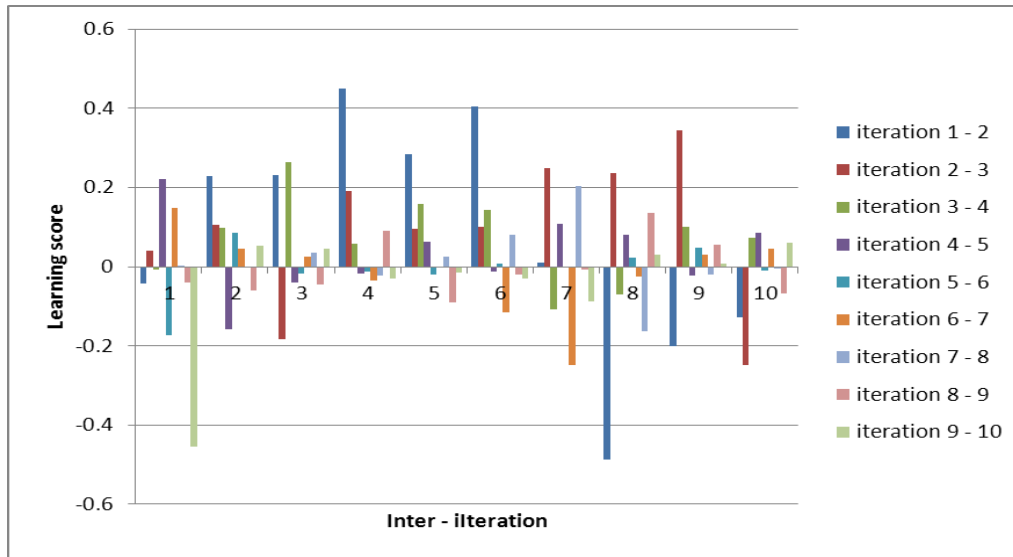


Figure 16. Learning factor on trust scores for each agent.

Figures 17 to 22 have the same interpretations as for cooperation and trust cases.

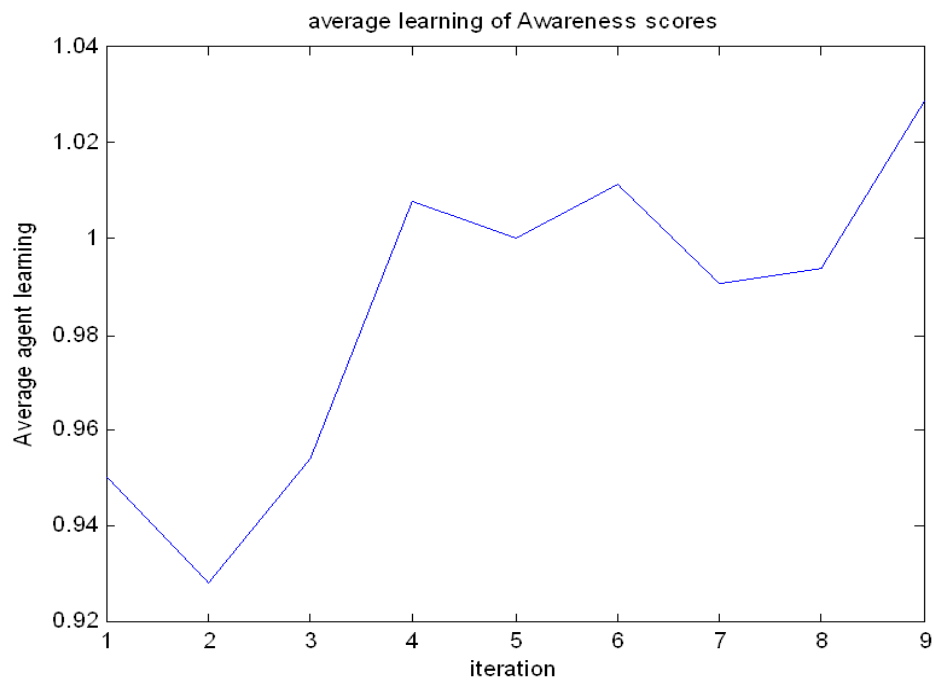


Figure 17. Evolution of average learning factor on awareness scores.

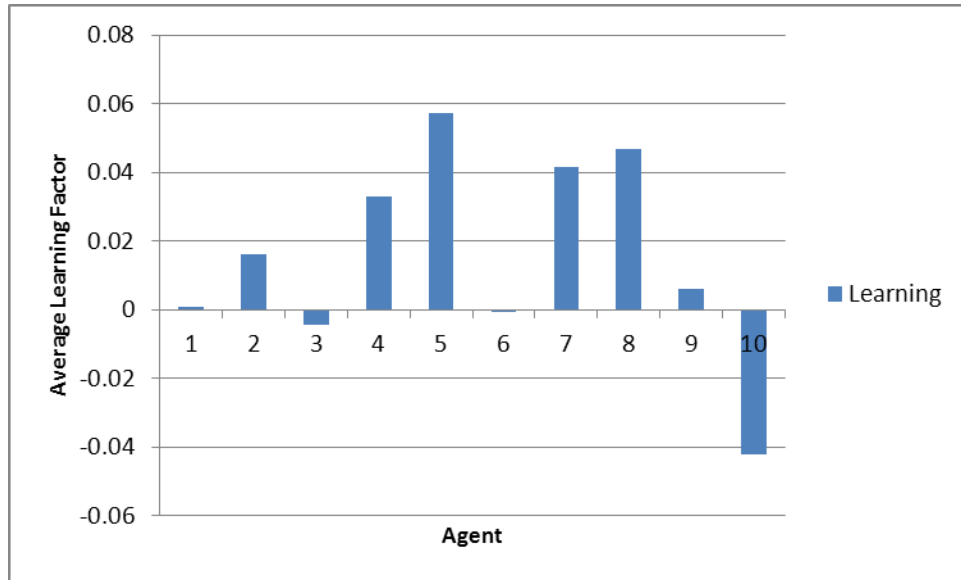


Figure 18. Learning factor on awareness scores for each agent.

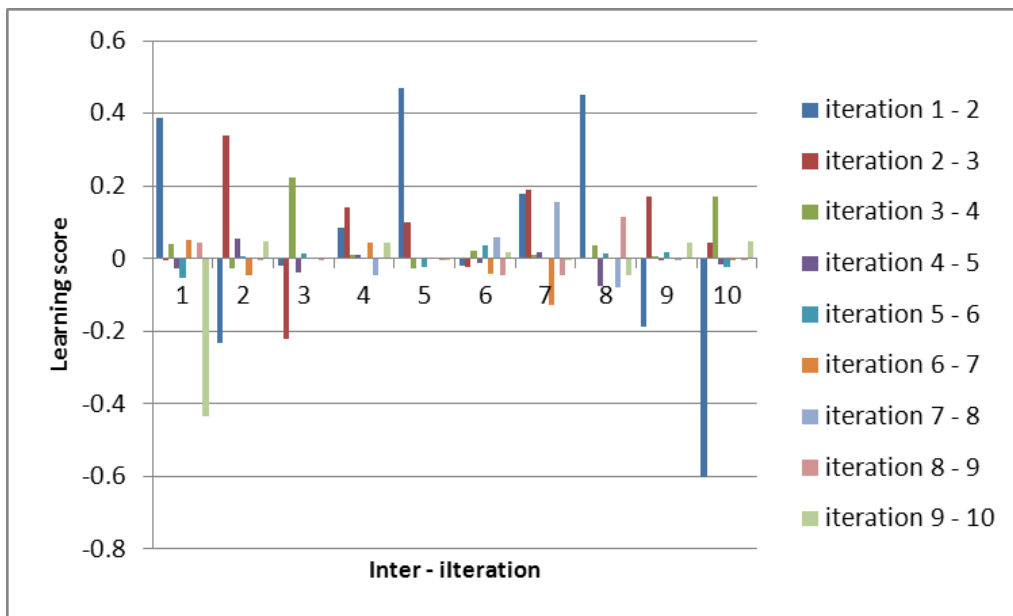


Figure 12. Learning factor on awareness scores for each agent.

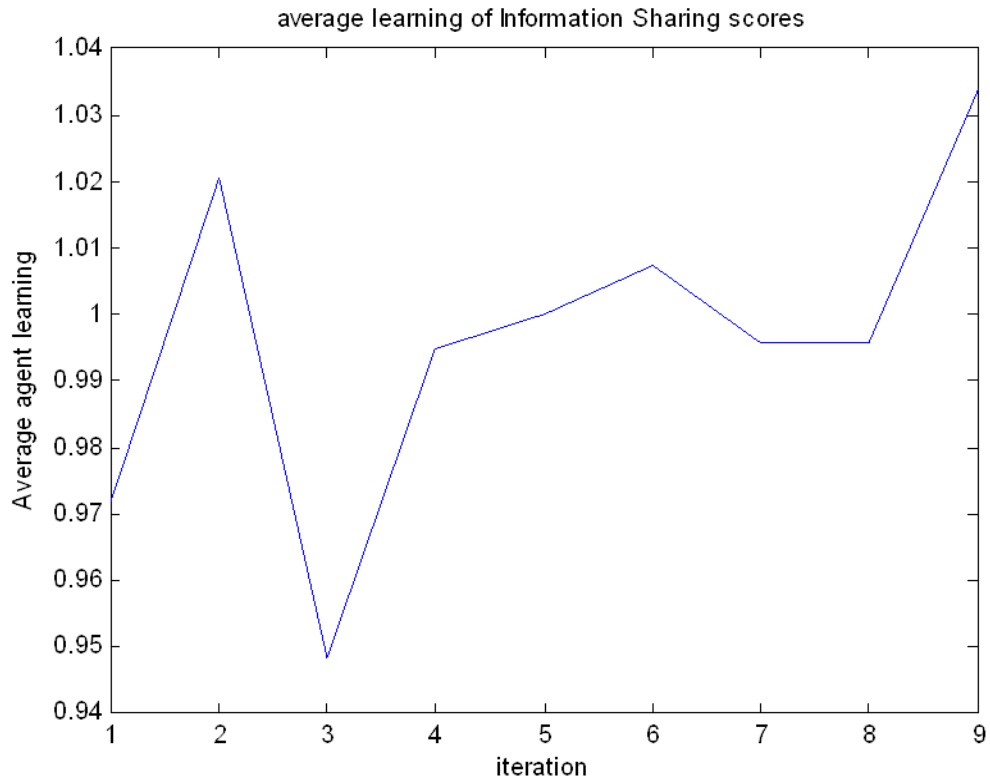


Figure 20. Evolution of average learning factor on information sharing scores.

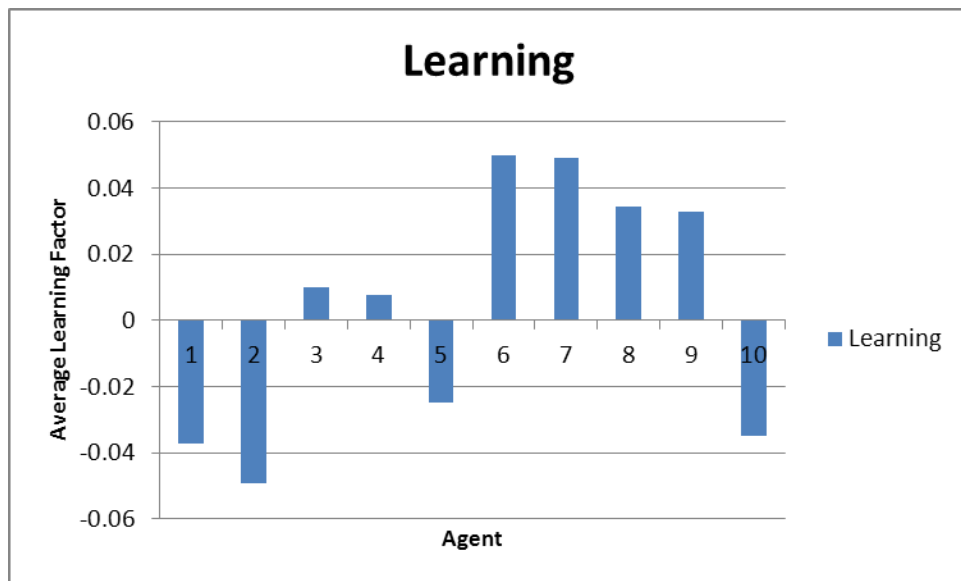


Figure 21. Learning factor on information sharing scores for each agent.

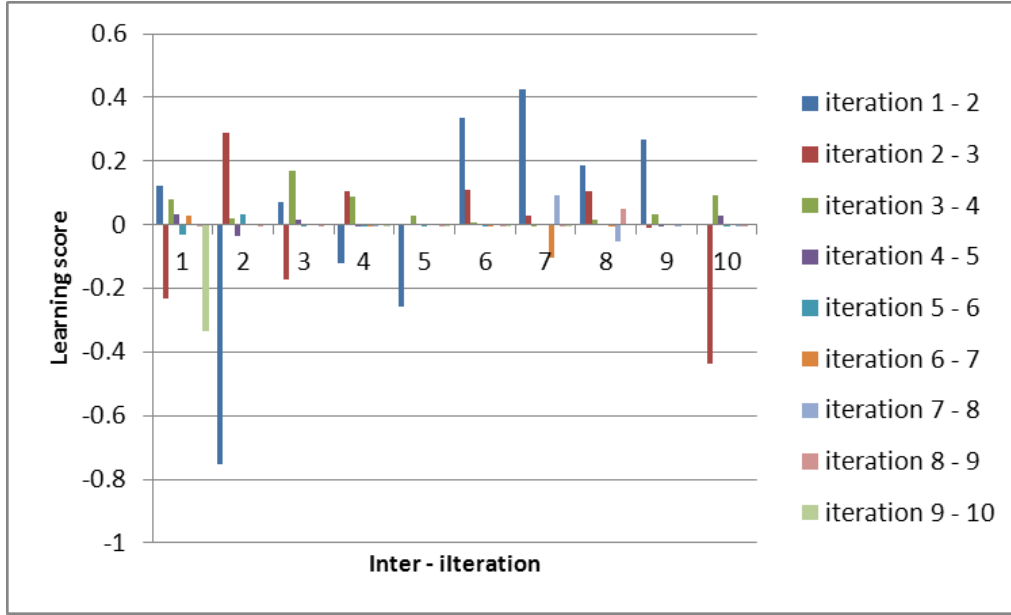


Figure 22. Learning factor on information sharing scores for each agent.

We conducted a Chi-squared test to examine for independence of the sociometric scores (cooperation, trust, awareness and information sharing) and monotonic of learning (decreasing or increasing). For this test, we conducted the simulation for 99 agents and calculated the learning for each sociometric score. Table 12 is a summary of the observed and calculated expected frequencies. The result shows that agent learning on each of the sociometric scores is not independent ($\chi^2_{0.05,3} = 7.815 < 109.58$; $p = 0.013$). The result indicates that there are some dependencies on how agents perceive other agents with respect to the sociometric scores. For example, the increase or decrease of trust between agents may change over time because of many circumstances, such as task changes, or new environmental information. Specifically, a change in an individual sociometric score may influence an agent's perception of other sociometric scores.

Table 12. Contingency table of learning versus sociometric scores

Learning	Cooperation	Trust	Awareness	Information Sharing	Total
Increasing	554(486.25)	543(486.25)	500(486.25)	348(486.25)	1945
Decreasing	436(503.75)	447(503.75)	490(503.75)	642(503.75)	2015
Total	990	990	990	990	3960

5.3 Adaptation by MANET Agents

Adaptation is the ability of agents to respond to new environmental stimuli. With respect to the sociometrics, an agent may encounter an unexpected difficult task environment due to degraded network system and must adjust its resources wisely in order to adapt to the new situation. More so, because of interaction with other agents, other agents can aid an agent facing new environmental constraints because they trust each other. They can share information on new environments, and can provide

cooperation to enable the affected agents to cope with the challenges. Thus, as the environment is changed, MANET agents should adapt to such environment by scaling their respective behaviors and perception of other agents to meet such changes.

Adaptation can be accomplished by agents using an evaluative feedback model from learning past actions and/or by using an on-going environmental niche to reorganize its behavior. In this respect, Biskupski, Dowling, and Sacha (2007) note as follows:

“The local agent environment can be modified by actions of the agent itself and actions of other agents operating in it. However, there is an uncertainty in the outcome of agent actions on the state of the environment due to a lack of knowledge of other agent actions as well as nondeterminism and dynamism of the environments”.

Salazar, Rodriguez-Aguilar and Arcos (2008) proposed a computational self-adapting mechanism that facilitates agents to distributively evolve their social behaviors (in our case, sociometrics) to reach the best social conventions. Their approach is borrowed from the social contagion phenomenon. Social conventions are akin to infectious diseases that spread them-selves through members of the society. With this, they show experimentally that a multi-agent system can either self-regulate or co-regulate specific social behaviors to cope with a dynamic environment.

With reference to the above observations, adaptation is important to MANET agents for many reasons, namely,

- (1) Due to the dynamic nature of MANET elements, a key challenge is the evaluation of mobility patterns and responses of the MANET agents (nodes) to changes in assigned tasks and their environments,
- (2) The need to encourage conflict resolutions and enhance cooperation and,
- (3) The possibility that nodes can change—new nodes entering a MANET system or nodes leaving due to an attack by an enemy action; In this case, an adaptation is needed for the MANET system to reorganize.

Soni and Dawra (2007) note that “self-organizing systems of agents with emergent system-level functions offer these features, but it is often far from obvious how the individual agent processes need to be designed to meet the overall design goal”. For example, agents must exchange information if they are to self-organize. This is an aspect of the sociometrics for MANET.

Adaptation by MANET agents deals with how each agent responds to the environment and perception by other agents. As such, adaptation is implemented in terms of a follower algorithm, where each agent chooses another agent to follow during movement. The follower algorithm is shown in Exhibit 3:

Exhibit 3. *The follower algorithm for sociometric adaptation*

Algorithm

Inputs:

Network in term of its connectivity matrix,

Number of iterations, N .

$k = 0$

1. While $k < N$
-

2. For each node n in the network, select a node m_n in the neighborhood to follow.

For each node n in the network generate:

an initial action a_n (step up, down, left or right);

a decision-making style $0 \leq d_n < 1$

3. For each node m , /* execution of action a_m .

4. Generate a random number r

For each node n in the network:

If $r \leq d_n$

Execute a_n

Else

Execute a_{m_n}

5. End if

6. End for

7. End for

8. End for

9. $k = k + 1$

10. Go to 3.

11. End Select

12. **End while**

In the algorithm above, the initial action follows the nearest neighborhood, which allows the agent to access information nearest to its location. The decision-making style $d_n \in [0,1]$ gives for each agent a threshold that helps it to decide whether to execute the action it selects or to execute the action of the other agent he is following.

We implemented this algorithm in MATLAB 7.8.0 for 10 agents, five actions and 11 iterations. Table 13 shows the selection of agents and the agents followed. Figure 23 is a bar graph, which compares the agents following behaviors.

The result shows that agent 5 was most followed and agent 10 was the least followed. Another observation from Figure 5.13 is that agents 1, 2, 3, and 4 are more followed compare to agents 6, 7, 8, and 9.

Table 13. Number of times agent is selected

Agent	1	2	3	4	5	6	7	8	9	10
Begin simulation	12	9	10	13	13	14	7	11	10	11
At the end of the simulation	13	10	11	17	21	11	5	8	9	5
Percentage of followers	8.33	11.11	10.00	30.77	61.54	0.00	0.00	0.00	0.00	0.00

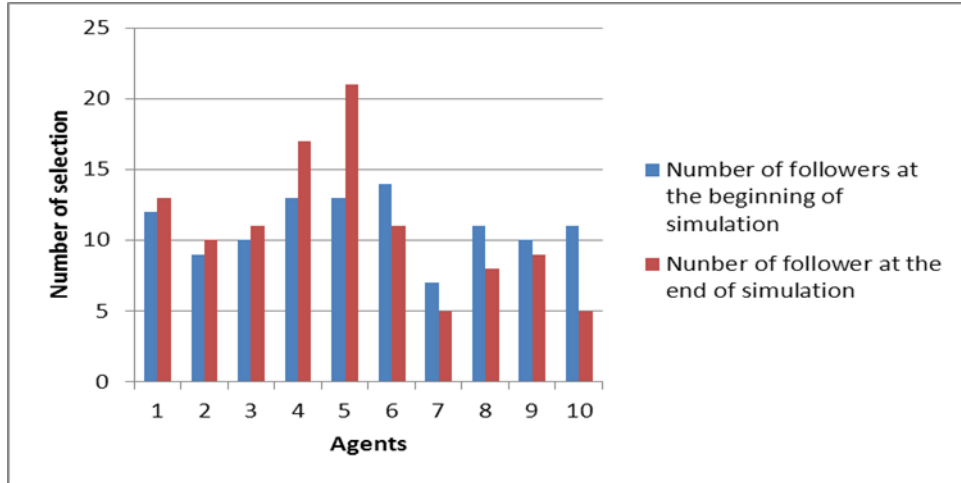


Figure 23. Comparison of action selection.

Figure 24 shows the bar chart of the frequency of action selections. Action d was selected 37 times.

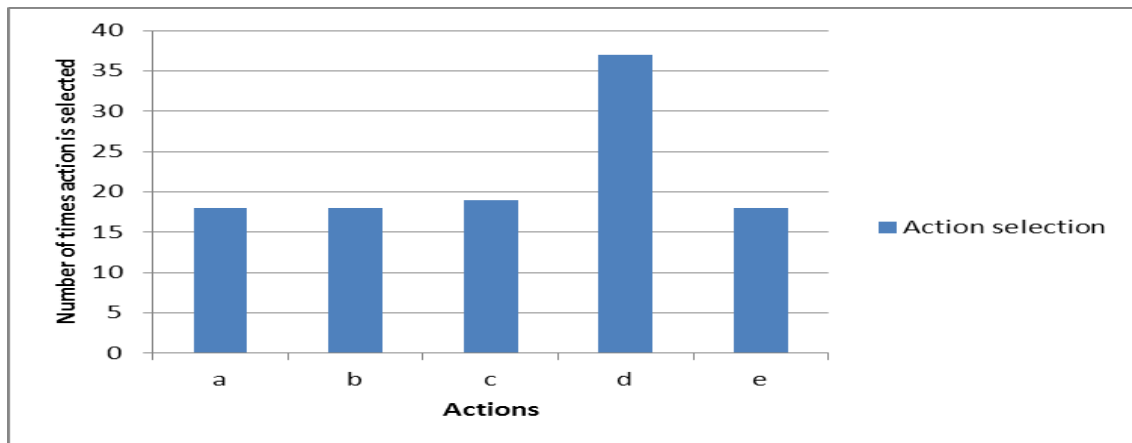


Figure 24. Frequencies of action selection.

5.4 Chapter Summary

This Chapter provides a sensitivity analysis for a MANET sociometric behaviors using learning and adaptation policies. The learning model is characterized and derived by assuming that each agent in the MANET system can accommodate changes in its environment. This includes its behavioral changes or perception of other agents based on a sociometric scale. For example, a learning score can be negative, zero, or positive. A negative score simply means that an agent has a reduced perception of other agents on the sociometric scales, a zero score means no change of opinion, and a positive score means a possible increase on the sociometric scales.

Through a simulation analysis, it was found that Agent 10 had the worst decrease in perception of other agents on the sociometric score (0%). Agent 1 had a decrease in three scales except for situation awareness (25%); Agents 2, 5, 8, and 9 had 75% learning

scores; Agents 3, 4, 6, and 7 had 100% learning scores—meaning that they improved on their perception of other agents on the sociometric scales.

With adaptation, a heuristic model was developed based on “agent-follow-agent (AFA)” algorithm with embellished neighborhood search algorithm. The simulation of AFA algorithm indicated that Agent 10 was not receiving any followers (0% adaptation). This means that Agent 10 does not have any trust, cooperate, or willing to share information with other agents. Agent 5 was the most followed with 61.54%. Any increase on followership score indicates the ability of an agent to adapt to the environment as well as perceiving other agents with increase sociometric scores. It also has some impacts on how actions are selected by a MANET node.

CHAPTER 6

A LABORATORY SIMULATION DEMONSTRATION

6.1. A MANET Configuration

The second part of the simulation experiments was developed to mimic MANET behaviors in real-time. Three computers with one user in each were used to simulate the environment. The computers were geographically dispersed within our laboratory to serve as different MANET nodes. Figure 25 shows an example screen capture of a user as a node simulating a MANET of three nodes (computers). In Figure 26, two MANET nodes (users) and a command and control (C2) are configured as shown on the upper part. The lower part of Figure 26 shows a sample window that captures the agent (Node) information in real-time. Figure 27 shows an example of how the simulation model recognizes an intruder by asking for node entry verification. Figure 28 shows MANET agents detecting an enemy intruder.

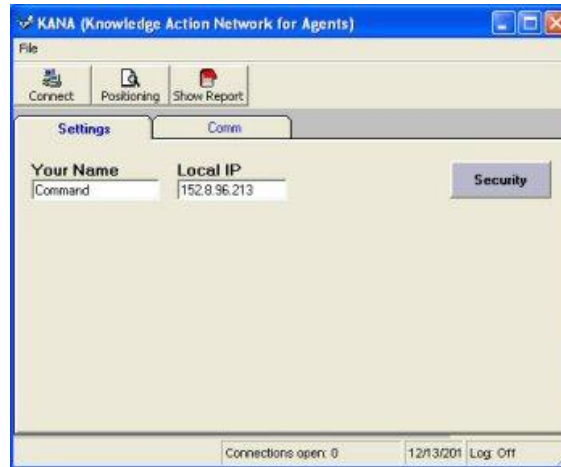


Figure 25. A MANET log-in screen

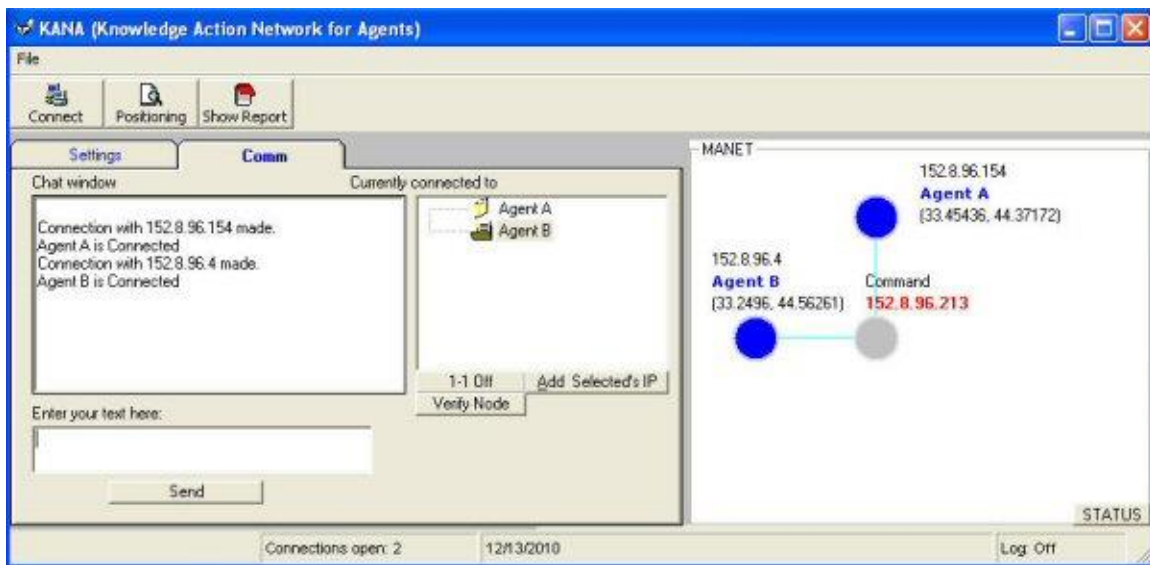


Figure 26. A MANET log-in screen with information sharing among agents

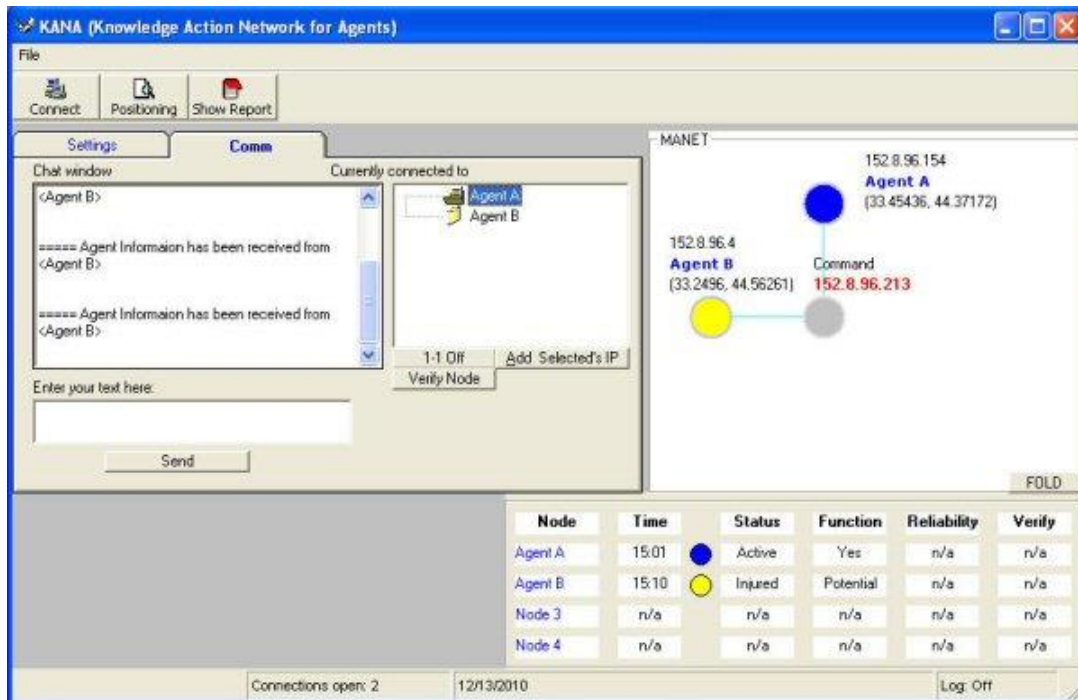


Figure 27. A sample MANET agent allowing authentication.

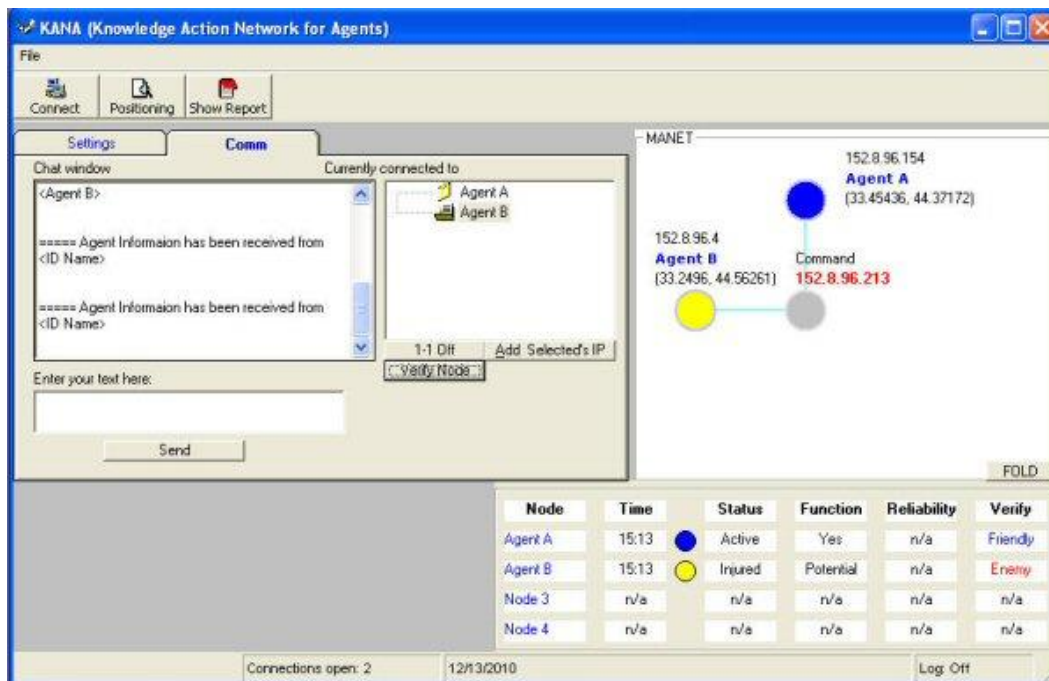


Figure 28. A network intrusion detection and verification by MANET agents

6.2. Observations and Sensitivity Analysis

By using the original node intrinsic ratings, the simulation model was analyzed to determine the effects of probability of enemy attack on the nodes. The levels of attack

are: low (5%), medium (10%) and high (20%). The average results showing the perception of contributions of the variables to overall system effectiveness are shown in Table 14. Table 14 data is also shown in Figure 29.

Table 14. Sample system level performance scores by intruder probability (%)

System performance	Low intruder probability (5%)	Med. intruder probability (10%)	High intruder probability (20%)
Trust	20.5	12.78	10.16
Cooperation	24.33	40.32	54.55
Awareness	28.97	21.23	15.12
Shared Information	26.19	25.67	20.17

The Student- Newman-Keuls test for significance at 5% level showed some differences between cooperation and trust across the levels of intrusion; there were no significant differences between cooperation and shared information; cooperation and awareness; and shared information and awareness. Also, there were significant differences between shared information and trust; and awareness and trust. The critical regions for student-Newman-Keuls were 16.75%, 20.76%, and 23.27% for means at 2, 3, and 4, respectively.

As shown in Table 14 and Figure 29, perception of trust and self-awareness decrease as intruder access to the network increase. This result translates to an increase in cooperation between network agents (nodes). Buttyan and Hubaux (2001) observed that cooperation in self-organizing MANETs depend mostly on cooperation between nodes. Goldbeck (2006) in reviewing trust in worldwide webs noted that trust in networks with frequent failures and phishing credentials lead to frequent suspicion, and hence a lack of trust by the users. With respect to self-awareness, Bologna and Setola (2005) noted that self-awareness in battlefield networks are functions of the level of network technology degradation and situation awareness. Network users can predict their level of self-awareness with respect to degree of comfort when the networks have reputation to assist the user especially at unexpected difficult tasks. The distribution of shared information across the three levels of intruder probabilities revealed no significant differences between low and medium probability levels. However, as the probability of intruder increases, there is some evidence of decrease in information sharing across the nodes.

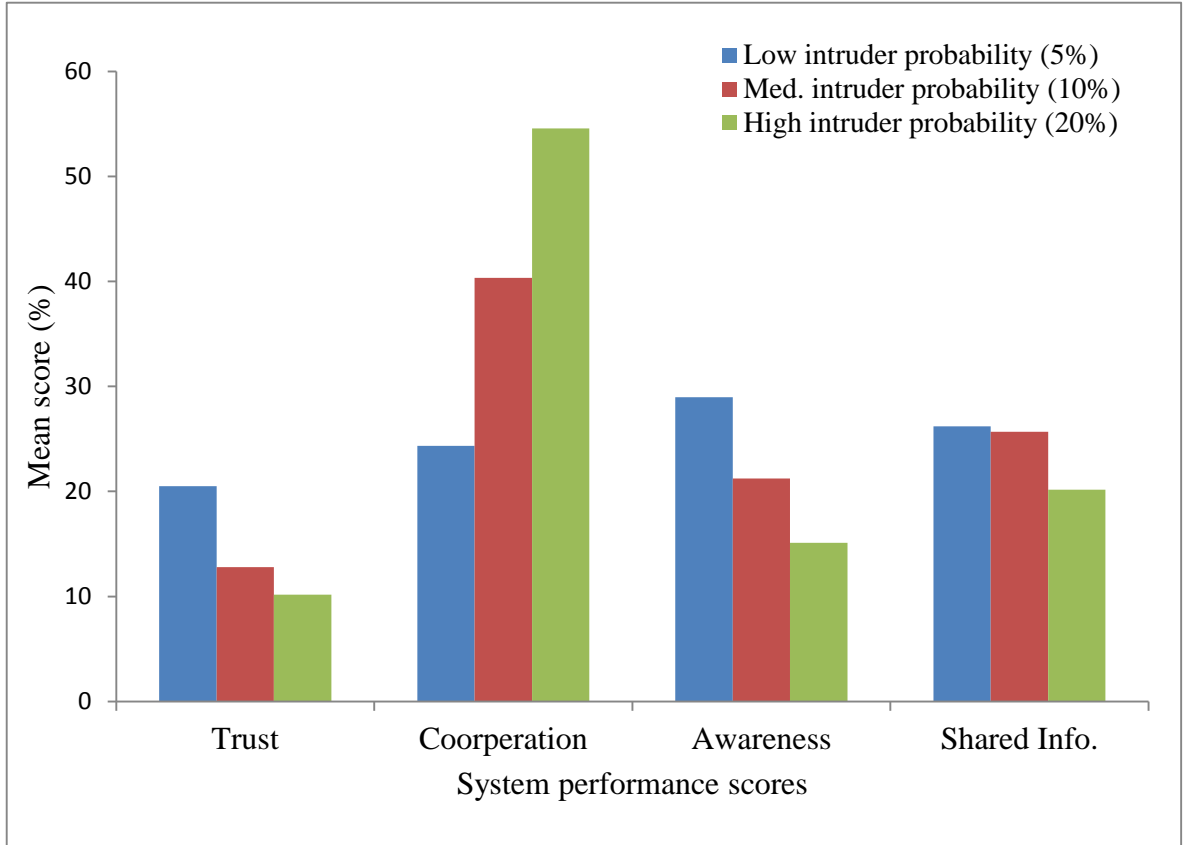


Figure 29. System performance distribution by intruder probability

6.3. Chapter Summary

This chapter mimicked a MANET behavior in a laboratory setting. We experimented on the socio-metrics developed in Chapter 4 with an extension how agents bind problems in context and provide solutions when faced with uncertainties and surprise such as those from non-authorized intrusion into the network. The focus was on how the socio-metric factors were used by the agents when they encounter external emerging behaviors as opposed to learning the factors through connectivity algorithms. We found that agent interacts and seek to self-organize when they experience a higher probability of intrusion into their domain. These issues are critical to the survivability of MANETS in battlefields. Thus, we can infer that when multiple entity behaviors interact, it is possible to derive emerging behaviors that make the functioning of MANET scalable across different echelons of information abstraction and control.

CHAPTER 7

SUMMARY, CONCLUSIONS, LESSONS FOR FUTURE RESEARCH

7.1. Summary and Conclusions

In **Chapter 1**, we introduce a MANET as a physics-based system as well as a socio-technical system. As a SoS, each node in a MANET is a system by itself—having the ability to adapt, takes actions, and make decision in any battlefield situation. With its multiple node configurations, connectivity is the main conduit of a MANET system and can be decomposed into subsystems, each with different operational behavior.

In **Chapter 2**, a brief literature related to modeling and simulation of MANET systems from both physical and human behavioral model perspectives is presented. It is observed that behavioral models are useful as MANETs seek to discover their neighbors through interconnection which are dependent on many social-behavioral factors such as trust and cooperation. An important joint physical and behavioral property of a MANET is its mobility. Two primary types of mobility are commonly used: entity models, where the single nodes move independently of each other; and group mobility models, where some of the nodes are forming groups. The mobility is governed by certain randomly occurring behavioral factors such as task attractors (e.g., enemy pursuit) and fear of being identified by adversaries. Recent efforts on MANET modeling and simulation is the use of bio-inspired natural phenomena or using artificial neural network (ANN) models to help agents to dynamically learn routes in the network.

Chapter 3 presents fuzzy-based agent models for modeling a MANET behavior. A MANET is represented and modeled as a symmetric $n \times n$ fuzzy matrix. An algorithm for calculating the evolutionary behaviors of MANET nodes using fuzzy product operations on the matrix is developed. It is shown that after a “sufficiently large number of iterations”, the fuzzy matrix converges to a “zero-one” matrix. The values of “0” and “1” simply means that two edges of the network with “1” have a crisp connectivity (and hence good communication), and those with “0” means no connectivity at all. This property is used in the simulation to control result convergence and simulation termination.

Chapter 4 presents the results of modeling and sample simulations using human behavioral traits with the sociometrics as the dependent variables. It is observed that as MANET nodes learned to know each other, the sociometrics tended to increase the connectivity with other nodes. Further observed is the fact that a decrease in values for Cooperation and Self-awareness do not mean that there is a decrease in how the nodes cooperated or had self-awareness. It simply means that nodes with high cooperation and self-awareness are likely to share information and create more trust in the network as time evolved. This was achieved by incorporating behavior updating mechanisms into the simulation model. The learning mechanism systematically trains nodes in the MANET system to cooperate, trust, share information, and have self-awareness by adjusting their individual achievement weights from the sociometric scores.

Chapter 5 presents the results of sensitivity analyses for a MANET sociometric behavior using learning and adaptation policies. The learning model is characterized and derived by assuming that each agent in a MANET can accommodate changes in its environment. This included its behavioral changes or perception of other agents based on a sociometric scale. A learning score can be negative, zero, or positive. A negative score simply means that an agent has a reduced perception of other agents on the sociometric scales, a zero score means no change of opinion, and a positive score means a possible increase on the sociometric scales. A heuristic model for behavior adaptation is introduced into the sensitivity analyses using an “agent-follow-agent (AFA)” algorithm. AFA’s concept is simply: nodes with lower sociometric scores will seek to imitate the behaviors of nodes with high sociometric scores. A selfish node will not receive a follower since it is insensitive to the needs of other nodes. For example, in our experiment, Agent 10 was not receiving any followers (0% adaptation). This means that Agent 10 does not have any trust, cooperate, or willing to share information with other agents. Any increase on followership scores indicate the ability of an agent to adapt to the environment as well as perceiving other agents with increase sociometric scores. It also has some impacts on how actions are selected by the MANET nodes, especially connectivity decisions.

Chapter 6 mimicked a MANET behavior in a laboratory setting. We experimented on the socio-metrics with an extension to how agents bind problems in context and provide solutions when faced with uncertainties and surprises such as those from non-authorized intrusion into the network. The focus was on how the socio-metric factors were used when they encounter external emerging behaviors as opposed to learning the factors through connectivity algorithms. We found that agents interact and seek to self-organize when they experience a higher probability of intrusion into their domain. These issues are critical to the survivability of MANETs in the battlefields. Thus, we can infer that when multiple entity behaviors interact, it is possible to derive emerging behaviors that make the functioning of MANETs scalable across different echelons of information abstraction and control.

Lessons Learned

The following lessons are derived from the pilot study:

- (a). It is important to consider human behaviors in modeling and simulation of MANET systems in order to obtain useful performance metrics similar to socio-technical systems.
- (b). By conducting sample simulations using human behavioral variables, we were to discover the influences of sociometrics values (trust, cooperation, self-awareness, and shared information) in a MANET behavior.
- (c). It is observed that as MANET nodes learned to know each other, the sociometrics variables tended to increase, and so is the connectivity with other nodes.
- (d). Further observed is the fact that a decrease in values for Cooperation and Self-awareness do not necessarily mean that there is a decrease in how the nodes cooperate or have self-awareness. It simply means that nodes with high cooperation and self-awareness were likely to share information and create more trust in the network as time evolved.
- (e). The AFA algorithm was able to point to certain tendencies of selfish behaviors. For example, a selfish node will not receive a follower. In our model, Agent 10 was not

receiving any followers (0% adaptation). Any increase on followership scores indicate the ability of an agent to adapt to the environment as well as perceiving other agents with increase sociometric scores.

(f). Experiments to mimic a MANET in the laboratory also gave some useful information useful for design. We found that the agents interact and seek to self-organize when they experience a higher probability of intrusion into their domain. These issues are critical to the survivability of MANETS in battlefields.

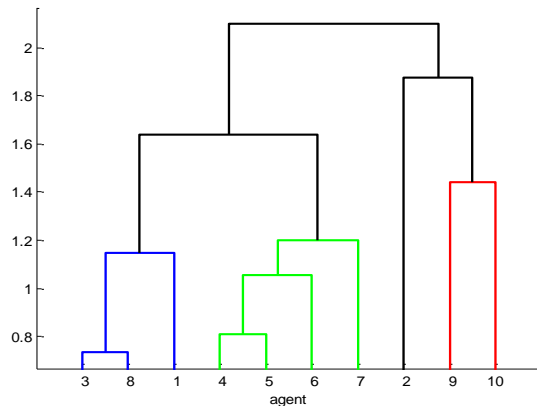
(e). The AFA algorithm was able to point to certain tendencies of selfish behaviors. For example, a selfish node will not receive a follower. In our model, Agent 10 was not receiving any followers (0% adaptation). Any increase on followership scores indicate the ability of an agent to adapt to the environment as well as perceiving other agents with increase sociometric scores.

(f). An experiment to mimic a MANET in the laboratory also gave some useful information useful for design. We found that the agent interact and seek to self-organize when they experience a higher probability of intrusion into their domain. These issues are critical to the survivability of MANETS in battlefields.

7.3. Suggestions for Further Research

The results of the study can be explored and validated for real-time battlefield applications. Some of the suggestions are:

1. **Investigate the use of probabilistically motivated cluster-based adaptation algorithm:** It is noted two agents can be close physically but disparate on the sociometric scale. we can study how similar or difference agents use their intrinsic and/or extrinsic properties to interact (See a fictitious diagram below).



2. **Quality of Service Measures:** Quality of service (QoS) is important in communication and information network. With the new framework for analyzing MANET behaviors, it will be nice to study the quality of service of MANET nodes as well as the MANET system itself. Noting that a MANET node broadcasts information to other nodes with trust, and knowing that some or not all

the information may get to the destination. A QoS can be computed using fuzzy sociometric scales discussed in Chapter 4. Informally, we propose a QoS model as follows:

$$QoS = \sum_{i \neq j} (p_i \otimes x_{ij}) \oplus (p_j \otimes x_{ji})$$

REFERENCES

- Abolhasan, M., Wysocki, T. and Dutkiewicz, E. (2004). A review of routing protocols for mobile Ad-hoc Networks. *Ad-hoc Networks* 2 (1) 1–22.
- Ammari, H. and El-Rewini, H. (2004). A location information-based route discovery protocol for mobile ad-hoc networks. *Proceedings of the IEEE International Conference on Performance, Computing, and Communications*, 625-630.
- Axelrod, R. (1984). *The Evolution of Cooperation*. Basic Books, Reprint edition, New York, 1984
- Benaissa M., Lecuire V., Syrotiuk V. R. and McClary D. W. (2004). ANOVA-informed decision trees for voice applications over MANETS. *Proceedings of the 6th IEEE International Conference on Mobile and Wireless Communication Networks*, (MWCN'04), pp 143-154.
- Biskupski, B, Dowling, J, and Sacha, J. (2007), Properties and Mechanisms of Self-Organizing MANET and P2P Systems. *ACM Transactions on Autonomous and Adaptive Systems*, 2 (1).
- Bologna, S and Setola, R (2005). The Need to Improve Local Self-Awareness in CIP/CIIP. *Proceedings of the 2005 First IEEE International Workshop on Critical Infrastructure Protection (IWCIP'05)*.
- Bowman, E.K. and Smith, J.A (2009). An analysis capability for system of systems research. ARL-SLAD, Aberdeen Proving Ground, MD.
- Buruhanudeen, S. M., Othman, B. and Ali, M. (2007). Existing MANET routing protocols and metrics used towards the efficiency and reliability- An overview. *Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications*, 14-17.
- Burt, R. (1992). *Structural Holes*. Cambridge, MA: Harvard University Press.
- Buttayan, L. and Hubaux, J.-P.(2001), “Nuglets: a virtual currency to stimulate cooperation in self-organizing mobile ad hoc networks,” Tech. Rep. DCS/2001/001, Swiss Federal Institute of Technology, January.
- Camp, T., Boleng, J. and Davies, V. (2002). A survey of mobility models for ad-hoc network research. *Wireless Communications and Mobile Computing (WCMC): Special issue on Mobile Ad-hoc Networking: Research, Trends and Applications*, 2(5) 483-502.
- Chiang, C.C. (1997). Routing in clustered multi-hop, mobile wireless networks with fading channel. *Proceedings of IEEE SICON_97*, 197–211.
- Chin, K. (2005). The behavior of MANET routing protocols in realistic environments. *Proceedings of the Asia-Pacific Conference on Communications*, Perth, Australia, 906-910.
- Cho, J-H. & Swai, A. (2009). Towards Trust-based Cognitive Networks: A Survey of trust Management for Mobile Ad Hoc Networks. In *14th Int'l Command and Control Research and Technology Symposium*, Washington D.C., U.S.A. (June 2009)
- Cioppa, T.M., Lucas, T.W., & Sanchez, S.M. (2004). Military applications of agent-based simulations. *Proc. Of the 2004 Winter Simulation Conference*. R.G Ingalls, M.D. Rossetti, J.S. Smith, and B.A. Peters (Eds.).

- Colagrosso M. D. (2005). A classification approach to broadcasting in mobile ad hoc network. Proceedings of the 2005 IEEE Conference on Communications (ICC'05), volume 2, pp 1112-1117.
- Daly, E. & Haahr, M. (2007). Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs. *MobiHoc '07*, September 9–14, 2007, Montréal, Québec, Canada.
- DaSilva, L.A. and Srivastava, V. (2004). Node participation in ad hoc and peer-to-peer networks: A game-theoretic formulation. Proceedings of Workshops on games and Emergent Behavior In Distributed Computing Environments.
- Deepa, S. & Kadhar Nawaz, D.M. (2010). A Study on the Behavior of MANET Routing Protocols with Varying Densities and Dynamic Mobility Patterns. *IJCA Special Issue on "Mobile Ad-hoc Networks"*, pp. 124-128.
- Dengiz, O. (2007). Maximizing Connectivity and Performance in Mobile Ad hoc Networks Using Mobile Agents. PhD Dissertation. Auburn University. Alabama, USA.
- Djenouri, D. & Badache, N.(2008). MANET: Selfish Behavior on Packet Forwarding. Encyclopedia of Wireless and Mobile Communications DOI: 10.1081/E-EWMC-120043599 Taylor & Francis, 576-587
- Dowling J., Curran E., Cunningham R. and Cahill V. (2005). Using feedback in collaborative reinforcement learning to adaptively optimize MANET routing. IEEE Transactions on Systems, Man and Cybernetics (Part A), Special Issue on Engineering Self-Organized Distributed Systems, 35: pp 360-372.
- Endsley, M.R. & Jones, W. M. (1997). Situation awareness, information dominance, and information warfare, Wright-Patterson AFB, OH: United States Air Force Armstrong Laboratory.
- Farago A., Myers A. D., Syrotiuk V. R. and Zaruba G. V. (2000), "Meta-MAC protocols: Automatic combination of MAC protocols to optimize performance for unknown conditions", IEEE Journal on Selected Areas in Communication, 18: pp 1670—1681.
- Frias-Martinez, V., Salvatore. J, Stolfo, S. J., & Keromytis, A.D.(2007). BARTER: Behavior Profile Exchange for Behavior-Based Admission and Access Control in MANETs. Information Systems Security: 5th International Conference (ICISS, 2009), Kolkata, India, December 14-18.
- Funge J., Tu X., Terzopoulos D (1999). Cognitive modeling knowledge, reasoning and planning for intelligent character. Proceedings of ACM SIGGRAPH99.
- Gaines, B & Ramkumar, M. (2008). A Framework for Dual Agent Routing Protocols for MANETs, IEEE Globecom 2008, New Orleans, LA.
- Goldbeck, J. (2006). Trust on the world wide web: a survey. Foundations and Trends in Web Science, 1(2), 23-36.
- Gong, W., You, Z., Chen, D., Zhao, X., Gu, M, & Kwok-Yan Lam, K-Y. (2009). Trust Based Malicious Nodes Detection in MANET. 978-1-4244-4589-9/IEEE
- He, L. and Wei, Y. (2008). A measure of mobility for evaluating mobile ad-hoc network performance. Proceedings of ICMMT2008, 3 1528-1531.
- Hui, P., Crowcroft, J., Yonek, E.(2008). BUBBLE Rap: Social-based Forwarding in Delay Tolerant Networks. *MobiHoc'08*, May 26–30, 2008, Hong Kong SAR, China: ACM 978-1-60558-073-9/08/05.

- Ishibashi, B. and Boutaba, R. (2005). Topology and mobility considerations in mobile ad-hoc networks. *Ad-hoc Networks*, 3 762-776.
- Kaaniche H. and Kamoun F. (2010), "Mobility Prediction in Wireless Ad Hoc Networks using Neural Networks", *Journal of Telecommunications*, 2 (1).
- Kaelbling, L. P., Littman, M. L., & Cassandra, A. R (1998). Planning and acting in partially observable stochastic domains. *Artificial Intelligence*, 101 pp. 99-134.
- Karhima, T. Lindroos, P. Hall, M. and Haggman, S.-G. (2005). A link level study of 802.11b mobile ad-hoc network in military environment. *Proceedings of Military Communications Conference (MILCOM 2005)*, vol.3, 2005, 1883- 1886.
- Kazantzidis M. I. (2005). MAC intelligence for adaptive multimedia in 802.11 networks. *IEEE Journal on Selected Areas in Communications*, 23: pp 357-368.
- Khatibi, S. & Rohani, R. (). Quorum-Based Neighbor Discovery in Self-Organized Cognitive MANET 21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communication. 978-1-4244-8016-6/10/\$26.00 ©2010 IEEE, 2234-2243
- Klewes, J., & Wreschniok, R. (2009). *Reputation Capital: Building and Maintaining Trust in the 21st Century* (Springer Heidelberg Dordrecht London New York).
- Knoester D. B., Goldsby H. J. and McKinley P. K. (2010). Neuroevolution of Mobile Ad Hoc Networks. *Genetic and Evolutionary Computation Conference, GECCO'2010* 603 – 610
- Kwak, B.J., Song, N.O. and Miller, L.E. (2003). A standard measure of mobility for evaluating mobile ad-hoc network performance. *IEICE Transactions on Communications* E86-B 3236-3243.
- Latour, B. (1987). *Science in Action: How to Follow Scientists and Engineers Through Society*. Milton Keynes: Open University Press
- Liu Y., Li Y. and Man H. (2005). Mac layer anomaly detection in ad hoc networks. *Proceedings of the 6th IEEE Systems, Man and Cybernetic (SMC) Information Assurance Workshop*, pp 402-409.
- Liu, Z., Joy, A. W., & Thompson, R.A (2004). A dynamic trust model for mobile ad hoc networks. *IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04)*, (Suzhou, Chine), May.
- Luo, X., Zhang, C., & Leung, H. (2000). Information sharing between heterogeneous uncertain reasoning models in a multi-agent environment: a case study, *International Journal of Approximate Reasoning*; v. 27, Issue 1, pp. 27–59.
- Macker, J. P., Chao, M., Mittu, R., & Abramson, M (2005). Multi-Agent Systems in Mobile Ad hoc Networks. *Military Communications Conference, MILCOM 2005*. IEEE 10.1109/MILCOM.2005.160579.
- Malpani N., Chen Y., Vaidya N. H. and Welch J. L. (2005). Distributed token circulation in mobile ad hoc networks. *IEEE Transactions on Mobile Computing*, 4.
- Marwaha S. and Indulska J. (2011). Context management system for pervasive WMN. *Seventh IEEE PerCom Workshop on Pervasive Wireless Networking*
- McClary D. W., Syrotiuk V. R. and Lecuire V. (2007). Adaptive audio streaming in mobile ad hoc networks using neural networks. *Ad Hoc Networks*.
- Mitchell T. (1997). *Machine Learning*. Boston: McGraw-Hill.
- Morgan, W. & Dilworth, R.P. (1939). Residuated Lattices, *Transactions of the American Mathematical Society*.

- Murthy, S. and Garcia-Luna-Aceves, J. J. (1996). An efficient routing protocol for wireless networks. *Mobile Networks and Applications* (Hingham, MA: Kluwer Academic Publishers) 1(2) 183 – 197.
- Musolesi, M. & Mascolo, C. (2007). Designing Mobility Models based on Social Network Theory. *Mobile Computing and Communications Review, Volume 11, Number 3*; 59-70.
- Ntuen, C. A. (2006). Cognitive Constructs and the Sensemaking Process. *Proceedings for 11th International Command & Control Research and Technology Symposium*. San Diego, CA.
- Pan Hui, P., Crowcroft, J., & Yoneki, E. (2008). BUBBLE Rap: Social-based Forwarding in Delay Tolerant Networks. *MobiHoc'08*, May 26–30, 2008, Hong Kong SAR, China.
- Penrose M. D., (1999). On k-connectivity for a geometric random graph. *Random Structures and Algorithms*, vol. 15, pp. 145–164.
- Perkins, C.E. and Bhagwat, P. (1994). Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers. *Computer Communications Review* 24 (4) 234–244.
- Pickman, C. H. (2008). A Low Cost Mobile Node Network Simulator. California State University, Long Beach. 147 pages
- Pirzada, A. A. & McDonald, C. (2004). Establishing trust in pure ad-hoc networks. In *Proceedings of 27th Australasian Computer Science Conference (ACSC'04)*, (Dunedin, New Zealand).
- Prema, G., Aravindan, C., Kannan, K., & Maheswaran, R. (2011). Empirical Modeling and Simulation of Temporal Based Adaptive Mobility Model for MANET. *Int. J. Communications, Network and System Sciences*, 2011, 4, 232-240
- Raghavan, V.N., Venkatesh, T., Peer, M.L., & Praveen, D.P. (2007). Evaluating performance of quality-of-service in large networks, *Proceedings of World Academy of Science, Engineering and Technology*, v. 20.
- Sabater, J. & Sierra, C. (2002). Reputation and social network analysis in multi-agent systems. *Proc. of AAMAS'02*, Bologna, Italy (July 15-19).
- Salazar, N, Rodriguez-Aguilar, J.A., and Arcos, J.L. (2008). An Infection-Based Mechanism for Self-Adaptation in Multi-Agent Complex Networks, *IEEE Computer Society*, 161-170.
- Shukla, D. (2001). Mobility models in ad-hoc networks, Master's Thesis, KReSIT-IIT, Bombay.
- Soni, D and Dawra, S (2007). AI System in (12th WSEAS Int. Conf. on Applied Mathematics, Cairo, Egypt, December 29-31, 2007 401.
- Sridhar, K.N. and Chan, M. C. (2005). Stability and hop-count based approach for route computation in MANET. *Proceedings of IEEE ICCCN*, 25-31.
- Srinivasan, V., Nuggehalli, P., Chiasserini, C.F., & Ramesh, R.R. (2003). Cooperation in Wireless Ad Hoc Networks, *IEEE INFOCOM*.
- Stepanov, I., Maron, P. J. & Rothermel, K. (2005). Mobility modeling of outdoor scenarios for MANETs. *Proceedings of the 38th Annual Simulation Symposium (ANSS'05)*, 312-322.
- Sun, W. Yu, Han, Z., & Ray Liu, K.J. (2006). Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks, *IEEE Journal on Selected Areas in Communications*, v. 24, no. 2.

- Sutton S. R. and Barto G.A.. (1998) . *Reinforcement Learning: An Introduction*. Cambridge, MA: MIT Press.
- Tan, D.S., Zhou,S., Ho, J-M., Mehta, J.S., & Tanabe, H (2002). Design and Evaluation of an Individually Simulated Mobility Model in Wireless Ad Hoc Networks. Communication Networks and Distributed Systems Modeling and Simulation Conference 2002.
- Theodorakopoulos, M., & Baras, J.S. (2006). On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks, *IEEE Journal on Selected Areas in Communications*, 24 (2), 318-328.
- Thomas, R.W., DaSilva, L.A., & MacKenzie, A.B. (2005). Cognitive Networks. *Proceedings of the 1st IEEE Int'l Symposium on New Frontiers in Dynamic Spectrum Access Networks*, 8-11, 352-360.
- Thompson, M.S., Mackenzie, A.B., DaSilva, L.A., & Hadjichristofi, G. (2012). A mobile ad hoc networking competition: A retrospective look at the maniac challenge, *IEEE Communications Magazine*, 50 (7), 121 – 127.
- Wei, W. & GuoSun, Z. (2010). Bayesian cognitive trust model based self-clustering algorithm for MANETs. *Information Sciences*, Vol. 53 No. 3: 494–505
- Wegner, C., Upton, S., Raffetto, M., Srivastava, N., & Oh, R (2006). Team 5: System-of Systems test Planning, I5-IDFW 14-Team 5, Naval Postgraduate, Monterey, CA.
- Wilson J. W. (2001). The importance of mobility model assumptions on route discovery, data delivery, and route maintenance protocols for ad-hoc mobile networks, Virginia Polytechnic Institute and State University.
- Wooldridge, M. J., N. (1995), "Intelligent Agents: Theory and Practice". *The Knowledge Engineering Review* 10 (2), 115-152.
- Vasantha , W.B., Smarandache , K.F., & K. Ilanthenral, K. (2007). *Elementary Fuzzy Matrix Theory and Fuzzy Models for Social Scientists*. Los Angeles: American Research Press.
- Venkatraman, S., Kumar, H.S., Sundarrajan, A., & Ramakrishna, M(2010). Reliability Improvement of Real-Time Data in MANET. *International Conference on Wireless Communication and Sensor Computing*.
- Vicente E. M. V., Dorgham S. and Radu P. (2005). NEURAL: A Self-organizing Routing Algorithm for Ad Hoc networks. *3rd International Symposium on Modeling and Optimization in Mobile, Ad-Hoc and Wireless Networks (WiOpt'2005)* 259 – 266.
- Virendra, M., Jadliwala, M., Chandrasekaran, M. & Upadhyaya, S. (2005). Quantifying trust in mobile ad-hoc networks. In *Proceedings of IEEE International Conference on Integration of Knowledge intensive Multi-Agent Systems (KIMAS'05)* (Waltham, USA), April.
- Younis, O., Kant, L., Chang, K., & Young, K. (2009). Cognitive MANET Design for Mission-Critical Networks. *IEEE Communications Magazine*.
- Younis, O., Kant, L., Mcauley, A., Manousakis, K., Shallcross, D., Sinkar, K., Chang, K., Young, K., Graff, C., & Patel, M. (2010). Cognitive tactical network models, *IEEE Communications Magazine*, 48(10), 70 – 77.
- Yu, T., Winslett, M., and K. E. Seamons, K.E. (2003). Supporting Structured Credentials and Sensitive Policies through Interoperable Strategies in Automated Trust Negotiation, *ACM Transaction on Information and System Security*, 6(1),

1-42.

Zhang, Y, Lee, W., & Huang, Y. (2003). Intrusion detection techniques for mobile networks, *Wireless Networks*, 9(5).

Zhou, L. (1999). Secure, Ad Hoc Networking. *IEEE Network*, 13(6), 24 – 30.

Zouridaki, C., Mark, B.L., Thomas, R.K., & Hejmo, M. (2006). Robust Cooperative Trust Establishment for MANETs. *Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria, VA, 30 October, 23-34.

APPENDIX A:

More Sociometric Simulation Results from Chapter 4

Table A-1. *Sample node characteristics input (Intrinsic)*

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
<i>Adaptation</i>	0.01	0.97	0.15	0.28	0.31	0.32	0.23	0.09	1.00	0.87
<i>RiskTaking</i>	0.10	0.88	0.42	0.80	0.73	0.47	0.87	0.80	0.32	0.43
<i>Dec – Mak</i>	0.62	0.83	0.54	0.80	0.53	0.39	0.13	0.71	0.05	0.17
<i>Awareness</i>	0.39	0.14	0.09	0.45	0.85	0.72	0.30	0.21	0.19	0.79
<i>Reputation</i>	0.64	0.14	0.85	0.24	0.20	0.48	0.28	0.85	0.52	0.04

Table A-2. *Sample relative rating matrix for cooperation (Extrinsic)*

Coop	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	1	0.07	0.86	0.84	0.56	0.19	0.87	0.22	0.31	0.83
A2	0.82	1.00	0.50	0.72	0.85	0.09	0.29	0.43	0.92	0.38
A3	0.57	0.41	1.00	0.10	0.40	0.05	0.94	0.20	0.25	0.19
A4	0.39	0.79	0.21	1.00	0.75	0.05	0.76	0.32	0.39	0.28
Coop	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A5	0.42	0.11	0.43	0.48	1.00	0.63	0.86	0.61	0.12	0.31
A6	0.28	0.96	0.88	0.39	0.11	1.00	0.25	0.65	0.88	0.12
A7	0.79	0.65	0.43	0.93	0.56	0.29	1.00	0.59	0.21	0.06
A8	0.49	0.53	1.00	0.61	0.35	0.12	0.66	1.00	0.19	0.30
A9	0.78	0.25	0.29	0.12	0.47	0.24	0.14	0.39	1.00	0.75
A10	0.79	0.14	0.93	0.25	0.47	0.29	0.61	0.26	0.69	1.00

Table A-3. *Sample relative rating matrix for trust (Extrinsic)*

Trust	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	1.00	0.31	0.23	0.03	1.00	0.06	0.57	0.09	0.09	0.67
A2	0.04	1.00	0.40	0.61	0.45	0.52	0.53	0.48	0.99	0.06
A3	0.81	0.25	1.00	0.14	0.87	0.04	0.18	0.88	0.84	0.25
A4	0.67	0.45	0.22	1.00	0.32	0.40	0.96	0.40	0.03	0.11
A5	0.92	0.75	0.48	0.52	1.00	0.75	0.25	0.94	0.47	0.09
A6	0.99	0.16	0.07	0.71	0.82	1.00	0.99	1.00	0.01	0.07
A7	0.81	0.26	0.06	0.59	0.58	0.29	1.00	0.18	0.21	0.59
A8	0.96	0.72	0.03	0.68	0.84	0.65	0.98	1.00	0.48	0.93
A9	0.73	0.99	0.80	0.95	0.94	0.02	0.11	0.11	1.00	0.23
A10	0.05	0.14	0.20	0.29	0.66	0.72	0.42	0.24	0.28	1.00

Table A-4. Sample relative rating matrix for awareness (Extrinsic)

Awareness	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	1.00	0.57	0.34	0.08	0.48	0.82	0.99	0.67	0.43	0.25
A2	0.68	1.00	0.07	0.50	0.48	0.59	0.45	0.79	0.53	0.52
A3	0.20	0.87	1.00	0.13	0.78	0.48	0.82	0.42	0.20	0.76
A4	0.67	0.59	0.50	1.00	0.01	0.51	0.86	0.03	0.06	0.56
Awareness	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A5	0.65	0.74	0.06	0.73	1.00	0.65	0.85	0.36	0.33	0.11
A6	0.22	0.50	0.74	0.53	0.17	1.00	0.20	0.11	0.97	0.68
A7	0.66	0.38	0.91	0.19	0.66	0.94	1.00	0.89	0.40	0.31
A8	0.32	0.16	0.38	0.89	0.31	0.07	0.91	1.00	0.39	0.11
A9	0.41	0.70	0.08	0.37	0.19	0.82	0.16	0.82	1.00	0.59
A10	0.14	0.94	0.08	0.82	0.84	0.78	0.12	0.50	0.89	1.00

Table A-5: Sample relative rating matrix for information sharing (Extrinsic)

Info Sharing	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	1.00	0.37	0.99	0.08	0.96	0.61	0.55	0.75	0.38	0.68
A2	0.43	1.00	0.96	0.87	0.13	0.11	0.49	0.63	0.09	0.96
Info Sharing	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A3	0.61	0.12	1.00	0.15	1.00	0.82	0.60	0.93	0.54	0.56
A4	0.54	0.53	0.57	1.00	0.89	0.74	0.39	0.59	0.44	0.63
A5	0.98	0.44	0.39	0.38	1.00	0.98	0.99	0.63	0.42	0.92
A6	0.09	0.41	0.66	0.26	0.53	1.00	0.08	0.34	0.64	0.10
A7	0.96	0.51	0.35	0.52	0.08	0.14	1.00	0.96	0.04	0.20
A8	0.34	0.58	0.80	0.86	0.72	0.67	0.89	1.00	0.29	0.40
A9	0.89	0.75	0.62	0.90	0.05	0.07	0.81	0.20	1.00	0.16
A10	0.33	0.10	0.06	0.75	0.19	0.81	0.81	0.46	0.08	1.00

A-1: Sample simulation results.

This section presents sample simulation results based on the sample input data. The results presents summary of statistics in each socio-metric at each simulation step. The first iteration result is:

System level sociometrics:

Cooperation: 30.3%

Trust: 17.3%

Situation Awareness: 14.5%

Information Sharing: 20.7%

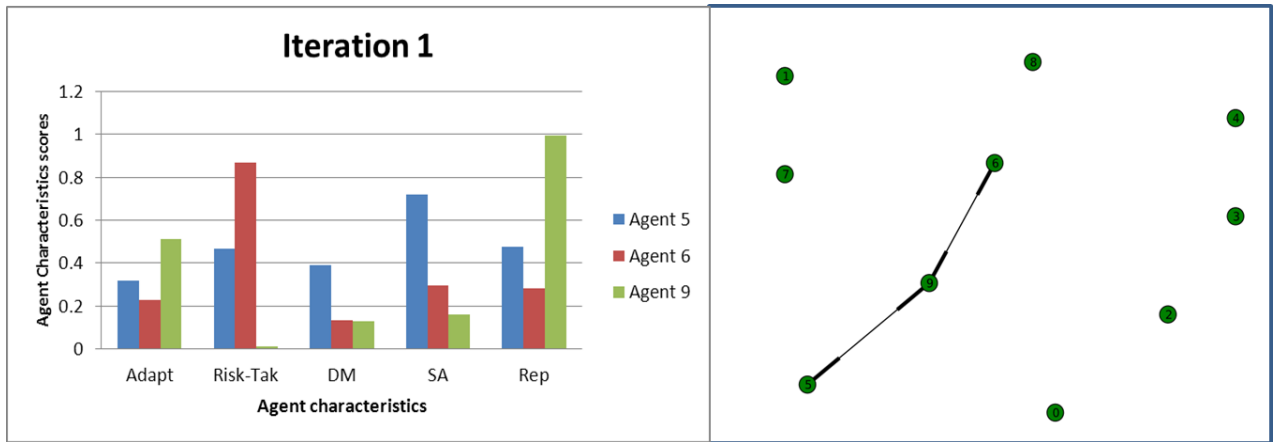


Figure A-1. Network physical configuration and graph of agent characteristics at iteration 1.

As shown in Figure A-1, agents 5, 6 and 9 are connected while other agents operate without any association with others. Tables A-6 to A- gives the updated matrix for each extrinsic score at each iteration.

Table A-6. Network Cooperation scores at iteration 1.

Coop	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	0.79	0.79	0.69	0.72	0.79	0.69	0.48	0.65	0.79	0.38
A2	0.64	0.64	0.61	0.64	0.56	0.33	0.64	0.61	0.36	0.36
A3	0.68	0.46	0.68	0.46	0.47	0.40	0.61	0.43	0.68	0.68
A4	0.66	0.65	0.54	0.66	0.56	0.29	0.66	0.59	0.54	0.54
A5	0.50	0.65	0.65	0.48	0.64	0.65	0.64	0.65	0.65	0.50
A6	0.56	0.83	0.83	0.51	0.47	0.83	0.56	0.65	0.83	0.56
A7	0.54	0.50	0.54	0.54	0.68	0.63	0.68	0.61	0.50	0.54
A8	0.57	0.41	0.79	0.34	0.45	0.34	0.79	0.34	0.45	0.45
A9	0.42	0.53	0.53	0.43	0.43	0.53	0.43	0.53	0.53	0.33
A10	0.60	0.60	0.80	0.61	0.60	0.38	0.66	0.80	0.60	0.38

Table A-7. Network trust scores at iteration 1

Trust	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	0.69	0.79	0.40	0.69	0.69	0.69	0.69	0.69	0.79	0.48
A2	0.64	0.61	0.36	0.61	0.61	0.61	0.64	0.61	0.48	0.61
A3	0.46	0.45	0.40	0.46	0.66	0.68	0.46	0.40	0.40	0.68
A4	0.66	0.37	0.37	0.59	0.58	0.54	0.66	0.37	0.37	0.59
A5	0.65	0.64	0.48	0.65	0.65	0.65	0.65	0.65	0.47	0.50
A6	0.83	0.51	0.47	0.71	0.82	0.83	0.83	0.83	0.48	0.56
A7	0.68	0.68	0.48	0.52	0.68	0.68	0.54	0.68	0.47	0.54
A8	0.79	0.32	0.79	0.34	0.79	0.45	0.42	0.79	0.79	0.45
A9	0.53	0.43	0.43	0.53	0.53	0.53	0.53	0.53	0.43	0.25
A10	0.80	0.72	0.40	0.68	0.80	0.65	0.80	0.80	0.60	0.80

Table A-8. Network awareness scores at iteration1

Awareness	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	0.68	0.79	0.69	0.53	0.48	0.69	0.48	0.79	0.69	0.68
A2	0.64	0.38	0.64	0.61	0.64	0.64	0.64	0.64	0.40	0.36
A3	0.46	0.68	0.46	0.68	0.68	0.68	0.46	0.50	0.68	0.68
A4	0.66	0.54	0.66	0.54	0.66	0.66	0.66	0.66	0.54	0.54
A5	0.64	0.64	0.65	0.64	0.64	0.65	0.64	0.50	0.65	0.65
A6	0.41	0.56	0.74	0.56	0.56	0.83	0.51	0.51	0.83	0.68
A7	0.65	0.68	0.50	0.68	0.68	0.65	0.68	0.54	0.50	0.50
A8	0.32	0.79	0.79	0.45	0.78	0.48	0.79	0.45	0.45	0.76
A9	0.43	0.50	0.53	0.53	0.43	0.53	0.43	0.36	0.53	0.53
A10	0.60	0.60	0.38	0.80	0.48	0.59	0.80	0.80	0.53	0.52

Table A-9. Network information sharing scores at iteration1

Info sharing	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
A1	0.48	0.79	0.79	0.79	0.53	0.69	0.49	0.63	0.64	0.79
A2	0.64	0.58	0.61	0.61	0.61	0.61	0.64	0.64	0.34	0.40
A3	0.46	0.46	0.46	0.68	0.46	0.68	0.68	0.46	0.44	0.68
A4	0.66	0.51	0.37	0.54	0.31	0.54	0.66	0.66	0.31	0.54
A5	0.64	0.44	0.65	0.50	0.64	0.65	0.64	0.63	0.64	0.64
A6	0.47	0.51	0.66	0.56	0.53	0.83	0.56	0.51	0.64	0.56
A7	0.68	0.44	0.54	0.42	0.68	0.68	0.68	0.63	0.50	0.68
A8	0.61	0.34	0.79	0.45	0.79	0.79	0.60	0.79	0.54	0.56
A9	0.33	0.08	0.63	0.35	0.16	0.11	0.91	0.82	0.31	0.70
A10	0.16	0.70	0.09	0.37	0.49	0.44	0.28	0.05	0.48	0.98

Similarly, the statistics for each iteration follows from Figures A-2 to A-

As shown in the networks, the connectivity between nodes progress at each iteration and each of their respective intrinsic properties are updated. In Figure 4.44, nodes (agents) 2, 5, 6, and 9 are fully connected while others are not.

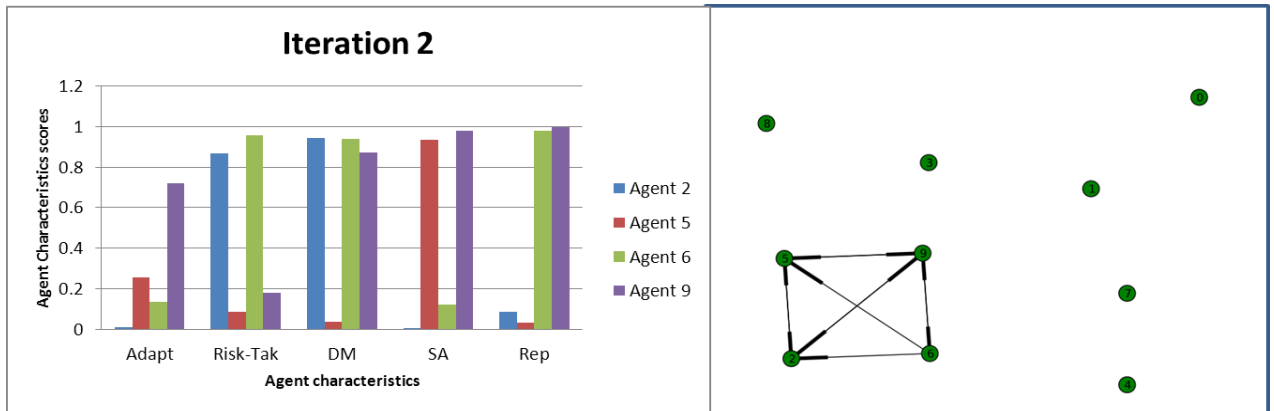


Figure A-2. Network physical configuration and graph of agent characteristics at iteration 2.

System sociometric scores:

Cooperation: 36.6%

Trust: 11.3%

Situation Awareness: 33.4%

Information Sharing: 26.8%

In Figure A-3, except for agents 0, 1, and 7, all others are fully connected.

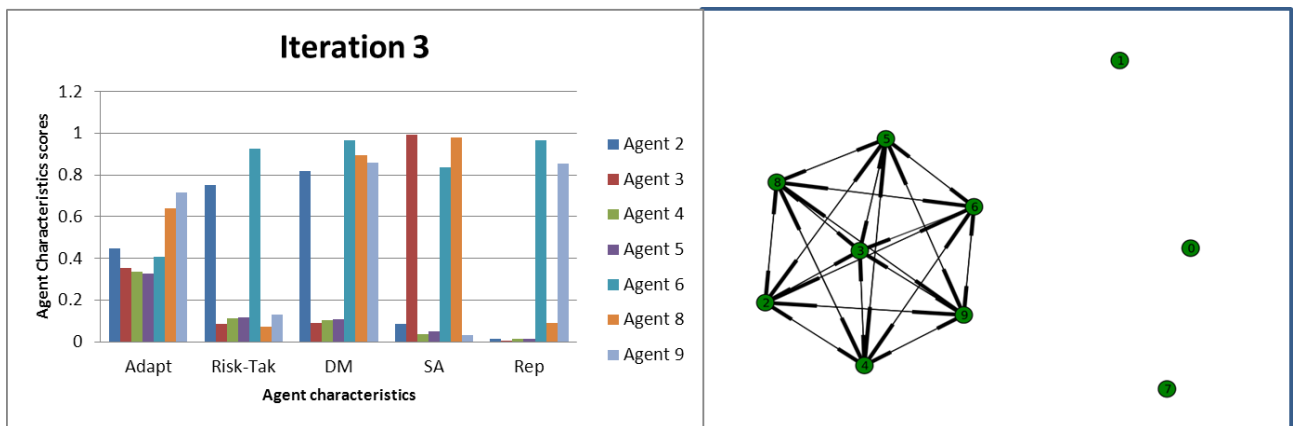


Figure A-3. Network physical configuration and graph of agent characteristics at iteration 3.

System sociometric scores:

Cooperation: 31.5%

Trust: 31.5%

Situation Awareness: 33.3%

Information Sharing: 34%.

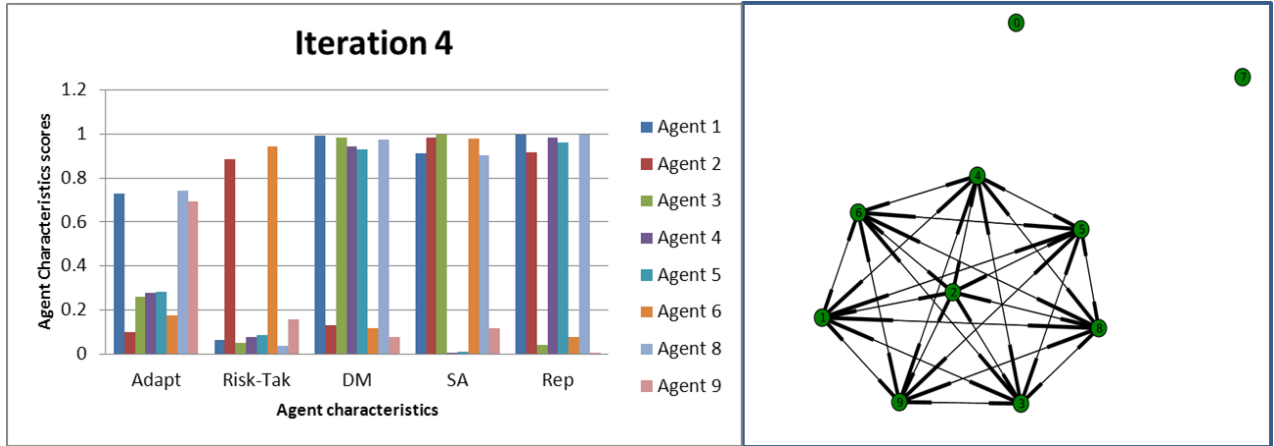


Figure A-4. Network physical configuration and graph of agent characteristics at iteration 4. In Figure A-4, only agents 0 and 7 are not connected to the rest of the nodes.

System level sociometric scores:

Cooperation: 31.0%
 Trust: 31.0%
 Situation Awareness: 31.6%
 Information Sharing: 33%

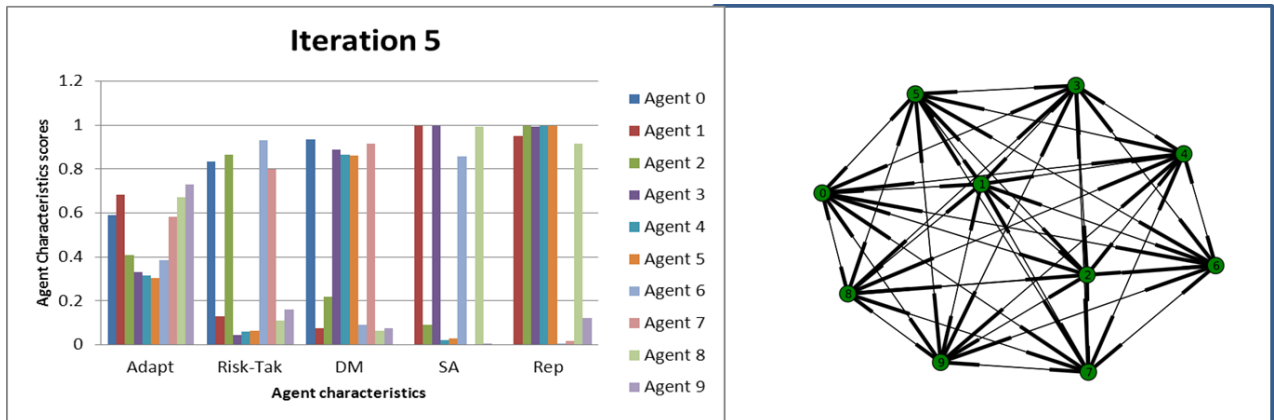


Figure A-5. Network physical configuration and graph of agent characteristics at iteration 5.

In Figure A-5, all nodes are fully connected. The process of iteration is continued until the network converging threshold for connectivity is achieved as shown in iteration 9 later.

System level sociometric scores:

Cooperation: 32.1%
 Trust: 32.1%
 Situation Awareness: 37%
 Information Sharing: 33%

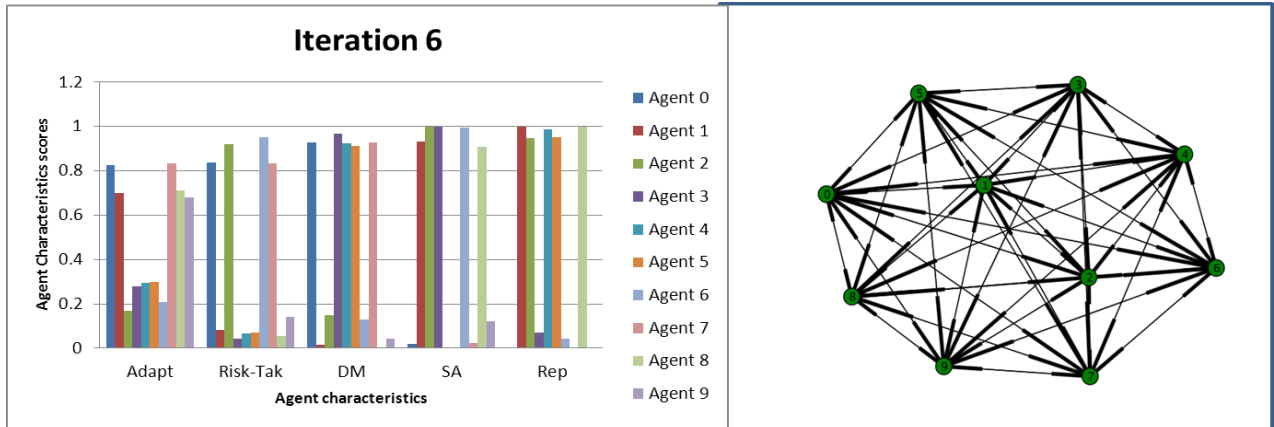


Figure A-6. Network physical configuration and graph of agent characteristics at iteration 6.

System level sociometric scores:

Cooperation: 31.9%

Trust: 31.9%

Situation Awareness: 32%

Information Sharing: 34.2%

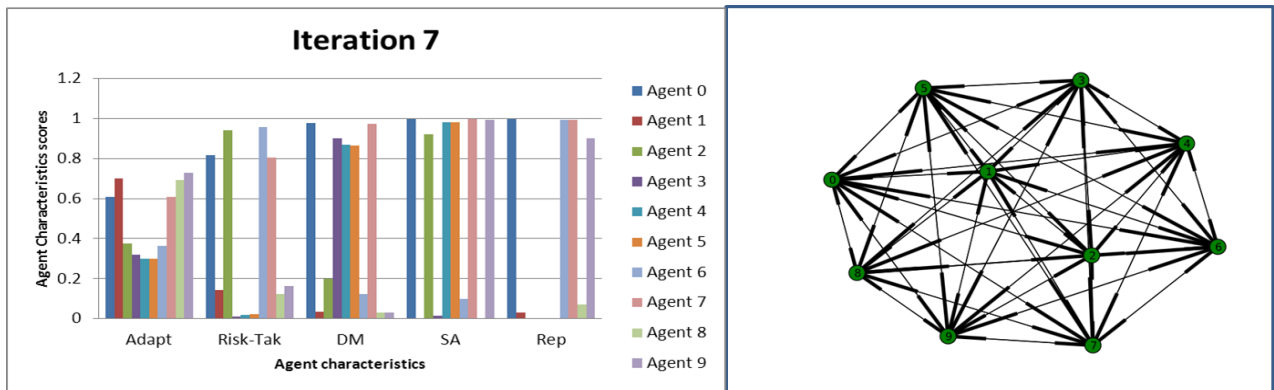


Figure A-7. Network physical configuration and graph of agent characteristics at iteration 7.

System level sociometric scores:

Cooperation: 32.9%

Trust: 32.9%

Situation Awareness: 37%

Information Sharing: 33%

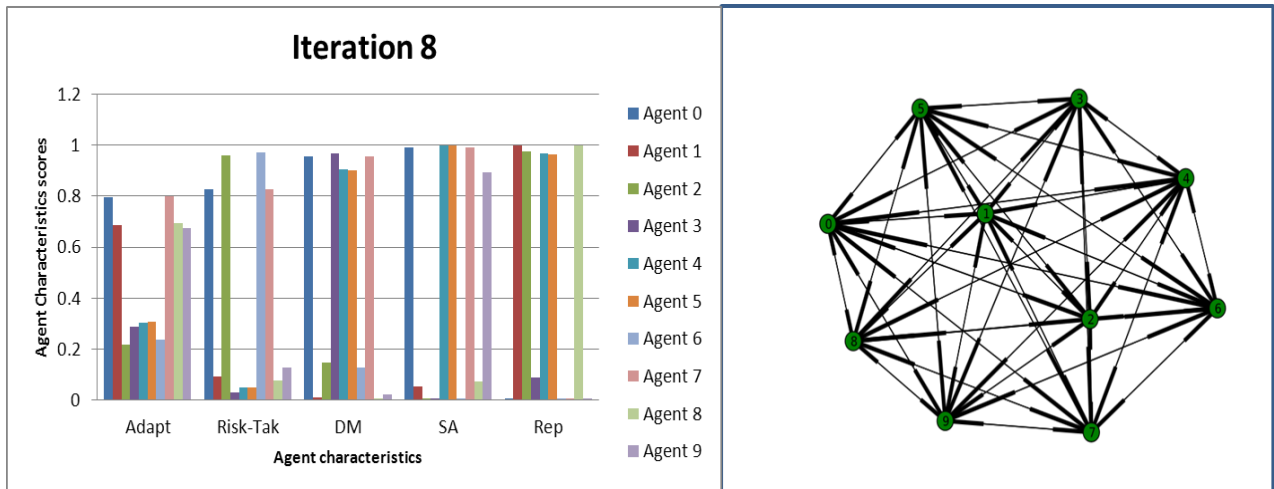


Figure A-8. Network physical configuration and graph of agent characteristics at iteration 8.

System level sociometrics:

Cooperation: 32.6%

Trust: 32.5%

Situation Awareness: 32.7%

Information Sharing: 33%

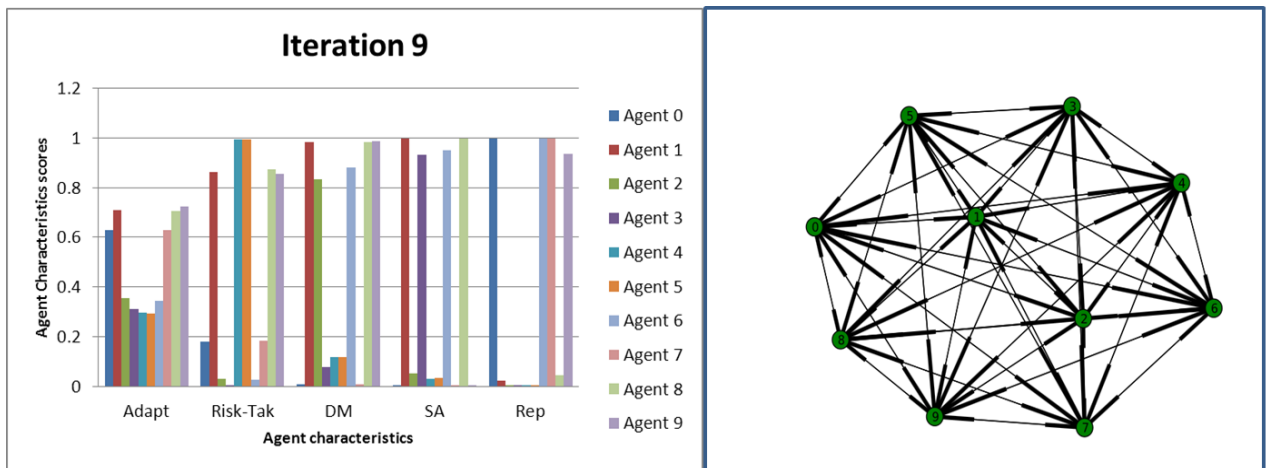


Figure A-9. Network physical configuration and graph of agent characteristics at iteration 9.

System level sociometric scores:

Cooperation: 33.2%

Trust: 33.2%

Situation Awareness: 37%

Information Sharing: 34.2%